Towards Implicit Learning of System-Assigned Authentication Tokens

by

Zeinab Joudaki

A Thesis Submitted in Partial Fulfillment
of the Requirements for the Degree of

Doctor of Philosophy
in
The Faculty of Business and IT
Computer Science

University of Ontario Institute of Technology

February 2018

Declaration

I hereby declare that except where specific reference is made to the work of others, the contents of this dissertation are original and have not been submitted in whole or in part for consideration for any other degree or qualification in this, or any other university. This dissertation is my own work and contains nothing which is the outcome of work done in collaboration with others, except as specified in the text and Acknowledgments.

Zeinab Joudaki
February 2018

Acknowledgements

My research and this thesis would not have been possible without the help and support of kind people around me; my supervisors, committee members, friends, family and my husband.

I would like to express my sincere gratitude to my thesis supervisors Prof. Julie Thorpe and Prof. Miguel Vargas Martin for their guidance, support and encouragement and for numerous conversations that have profoundly influenced my thinking about the subject of this thesis. The joy and enthusiasm you have for research was contagious and motivational for me.

I would also like to thank my supervisory committee who helped me during different stages of my research, Prof. Christopher Collins and Prof. Stephen Marsh. I would like to also thank my examiners Prof. Jeremy Bradbury and Prof. Mohammad Mannan for the comments and suggestions that improved this work.

I gratefully acknowledge NSERC for funding sources that made my Ph.D. work possible. The rest of funding was provided as scholarship, teaching and research assistantships I received from Faculty of Business and IT at UOIT.

I would like to thank my parents, family and many friends that made my life happier during these years. I appreciate your wise counsel and sympathetic ear. You are always there for me. And my very special thanks to my husband who stood by me through all ups and downs for these years of my study. He always cheered me up to motivate me work better.

Abstract

People tend to choose predictable passwords which are vulnerable to guessing attacks. To combat the security issue, system-assigned authentication keys were proposed, but this comes at a cost to memorability. In this thesis, I explore two different approaches to improve memorability of system-assigned keys through implicit learning: one that directly uses implicit memory alone, and another that indirectly uses implicit memory as a method to reinforce explicit memory.

I first explore the feasibility of direct implicit learning-based authentication secrets, *Tacit Secrets*: system-assigned passwords that you can remember, but cannot write down or otherwise communicate. I design an approach to creating Tacit Secrets based on *Contextual Cueing*, an implicit learning method previously studied in the cognitive psychology literature. My feasibility study involving 30 participants indicates that my approach has strong security properties: resistance to brute-force attacks, online attacks, classical phishing attacks, and some coercion attacks. It also offers protection against leaks from other verifiers as the secrets are system-assigned. My approach also has a high login success rate and low false positive rates. I explore the trade-offs of different configurations of my design and provide insight into valuable directions for future work.

In light of the promising results of Tacit Secrets, I propose a novel idea for training users system-assigned passphrases using implicit learning indirectly. Passphrases are passwords consisting of multiple words, initially introduced as more secure authentication keys that people could recall. Unfortunately, people's propensity is to choose predictable natural language patterns in passphrases, again resulting in vulnerability to guessing attacks. Making

them system-assigned would improve security, but at a cost to memorability. With the goal of improving the usability of system-assigned passphrases, I propose a new approach for reinforcing system-assigned passphrases by involving implicit memory. I design, implement, and test a system that employs this approach using two implicit learning techniques: contextual cueing and semantic priming. In an 880-participant online study, I explored the usability of 4-word system-assigned passphrases using the proposed approach compared to a set of control conditions. My results showed that the proposed approach improves usability of system-assigned passphrases, both in terms of recall rates and login time. This work sheds light into the potential of implicit learning for system-assigned authentication, suggesting it can improve its usability and therefore its feasibility.

Table of contents

List of figures

List of tables

Chapter 1

Introduction

Due to the prevalence of computer systems, the demand for providing confidentiality, integrity, and secure authentication for multiple accounts is escalating. Authentication can be defined as one entity proving its identity to another. The human factor is identified as a significant reason for many security solutions being compromised and attacks to be successfully conducted on systems. Security experts have proposed several security recommendations and solutions. Unfortunately, users continue choosing weak passwords that are vulnerable to guessing attacks, reusing passwords for different accounts [4, 5], writing down passwords, and exposing sensitive and important information on social media; these are pervasive examples of why attackers always target this weak link in the security chain.

The security of user-chosen passwords has become a serious concern to organizations and individuals alike. Dramatic improvements have been made in offline guessing (or trawling) attacks [6, 7] and targeted attacks that exploit a user's reused passwords [8]. The threat of these attacks is growing with the increasing amount of publicly leaked password data [9]. Perhaps the most damning are attacks that combine leaked password data with personal information—such online targeted password guessing attacks have been shown to guess over 32-73% of passwords within 100 attempts [10]. By simply crawling users' personal profiles on social networks, lots of private attributes of users can be inferred [11, 12], helping attackers to crack users' passwords [13].

One solution to this problem is using password creation policies as explicit guidance in order to increase security. These policies which include requirements for password length, composition of characters, and avoiding dictionary words, were initially proposed to improve security. However, these policies are not always enforced and users often ignore them [14]. Also, enforcement and incorporation of such policies results in less security due to limitations in human memory, as users tend to record these keys to recall them later. However, writing down passwords is only secure in some situations, e.g., when they are stored in a physically secured location such as a safe. Given all the aforementioned flaws, end-users continue to struggle creating and memorizing text-based passwords.

Password managers offer another solution to these problems by allowing users to generate and securely store random passwords. However, many users distrust them given recent password manager data breaches [15] and software vulnerabilities[16]. Yet another solution, for a small number of accounts is to assign users a random, *system-assigned* password; however, these are well-known to have significant problems with memorability [17] and thus users writing them down. This problem motivates my research into completely new approaches for system-assigned authentication secrets to provide resistance to online attacks, phishing attacks, and leaks from other verifiers.

The focus of this dissertation is on system-assigned authentication schemes enabled by implicit learning. I explore literature on implicit learning and identify a promising method called *Contextual Cueing (CC)*. In CC, users are trained to implicitly learn the location of a target item on a display full of many distractors. The use of CC and SP may also have interesting properties for accessibility. This benefit is granted to an authentication scheme when users are not prevented from using the scheme by disabilities or other physical (not cognitive) conditions [3]; for example, it has been found to remain intact in several neurological and mental disorders [18], and to work with subjects having dyslexia [19, 20].

Nerostro et al. [21] also studied how people with schizophrenia suffer from deficits in attentional control, they have executive function and controlled semantic retrieval. However, they have improved automatic processing, reflected by increased conscious and unconscious semantic priming [22, 23]. The unconscious mechanism of information processing and retrieval for the proposed approach makes it more accessible to users.

I first design and evaluate an approach, using implicit learning directly, called *Tacit Secrets*, for producing an authentication secret that the user can remember, despite the fact they cannot write it down. The positive 30-participant feasibility study results demonstrate that implicit learning can be used to produce a user authentication approach with high accuracy, and strong security properties, and as such might be employed in future authentication systems research. In particular, it indicates that the designed approach to Tacit Secrets has high authentication success rates (86-97%, depending on the performance metrics used), and low false positive rates (9.2-0.4%, depending on the performance metrics used). The false positive rate is high when a single metric (i.e., RT) is involved; however, by incorporating more distinctive features and testing different configuration of the approach we can further decrease this number. The security analysis indicates that the approach is resistant to offline guessing attacks, online guessing attacks, classical phishing attacks, and some types of coercion attacks. It is also resilient to targeted impersonation and leaks from other verifiers due to the Tacit Secret being system-assigned. Finally, it also provides some resistance to observation attacks and shoulder surfing, such that a successful attack would require multiple observations. Tacit Secrets could be used for any system requiring the strong security guarantees offered by system-assigned passwords.

In light of the promising results from Tacit Secrets, which directly uses implicit memory, I take advantage of implicit learning mechanisms indirectly to enhance memorability of system-assigned passphrases. This technique appears to improve the memorability of system-assigned authentication secrets. An 880-participant online study shows promising results in terms of recall rates when the designed training is compared to a set of control conditions.

The results showed 88% of the participants were able to successfully recall their assigned passphrases 7 to 8 days after they were assigned, which is significantly higher ($p < .001$) than the participants in the Control condition (56.94%). A nice side effect of the design is that it significantly reduced login times. The usability analysis also confirmed users' satisfaction of the proposed approach. Using a System Usability Scale (SUS) questionnaire, implicitly reinforced passphrases received a higher SUS score compared to other conditions, indicating promise of implicit learning as a tool for improving the usability of system-assigned authentication secrets. Implicitly Reinforced Passphrases could be used for any system requiring the strong security guarantees offered by system-assigned passwords.

For the rest of this chapter, I provide the thesis motivation, summary, and statement in Section 1.1, 1.2, and 1.3. My main contributions are also listed in Section 1.4.

1.1 Motivation

Text-based passwords are known as the most popular knowledge-based authentication (KBA) form. Given the choice, users tend to choose predictable patterns when creating passwords which compromise security. In response to the issues related to text-based passwords, many alternatives have been proposed for secure authentication. Although these methods could offer a high level of security, they are often suffering from usability issues.

System-assigned authentication schemes could provide the desired security; however, users tend to forget them or perform insecure coping behaviors in order to recall them [24]. A challenge is thus to provide users with secure authentication secrets without compromising memorability.

Memory research lies heavily on the distinction between explicit and implicit memory. Explicit (declarative) memory is based on conscious retrieval of previous facts and events whereas implicit (non-declarative) memory is related to unconscious recollection which results in improved performance of perceptual tasks. Researchers continue to find paradigms to dissociate explicit learning processes (related to verbalizable rules) from implicit learning processes (related stimulus–response associations that remain outside awareness). An important characteristic related to implicitly acquired knowledge is that it cannot be articulated as the memory traces for that is implicit. Numerous cognitive and neuropsychological studies have shown a variety of striking dissociations between implicit and explicit memory. An important difference between implicit and explicit memory is that implicit memory influences behavior in a less flexible but more durable way without consciousness. Employing implicit memory techniques provide can provide an efficient mechanism for encoding of system-assigned authentication secrets and such learning can facilitate memorization process and recalling them.

I explore use of implicit learning directly and indirectly to help users learn system-assigned authentication secrets. Implicit learning occurs as a result of internalizing the regularities that take place in the external environment. When knowledge acquisition occurs without conscious awareness, it is considered implicit [25]. Implicit learning allows the acquisition of complex information [26, 27] and appears to be more resilient than explicit learning. Many cognitive abilities can be impaired by severe head injuries; however, implicit learning is immune to injury due to its earlier development compared to explicit learning [28]. This learning mechanism will result in more durable and robust learning. The advantages of implicit learning are exciting as using it may help researchers improve the accessibility of authentication. My research makes use of two implicit learning mechanisms, known as *contextual cueing (CC)* and *semantic priming (SP).*

1.2 Thesis Summary

I designed new authentication approach to directly employ implicit learning using CC, whereby the arrangement of items on a 2-D display creates a *context.* A set of such contexts is what the user implicitly learns and becomes their secret key. CC is a robust effect shown to last after delays of at least 6 weeks [29, 30]. I use this mechanism to carefully design and implement an approach I call “Tacit Secrets”, authentication secrets you can recall but can’t write down or otherwise communicate.

Through an in-lab user study, I tested multiple configurations of my approach with and without eye-tracking information. I found that incorporating eye-tracking information produces substantial improvements in authentication success rate, training times, and login times.

I evaluate the accuracy and security of Tacit Secrets through an experiment, showing that it achieves much higher login success rates than another implicit learning based scheme reported in the literature [31]. Even without eye-tracking data, the proposed scheme successfully retrieves the implicitly learnt key 100% of the time immediately after training and 86% of the time one week later. I further analyze the proposed scheme by incorporating user’s eye-tracking data while performing the task. By adding two eye-tracking measures, I could reach higher success rates one week later for my approach (92.86%) and a lower authentication duration (maximum 1.5 minutes). This login time is considerably lower than the previously proposed purely implicit learning based authentication scheme [31]; moreover, given the substantial resistance to different attacks and specific use cases the approach can be applied for, the login time can be reasonable if the security is the main concern.

The feasibility study configuration employed a long training phase as done in earlier CC literature; however, we noticed learning was detectable in a much earlier time frame; thus we can possibly reduce the training time. It is worth noting that the proposed approach is not intended to be used for everyday authentication (e.g., e-mail accounts). Rather, it has potential for use in high security situations such as enterprise server administration or physical security. It may also prove useful for fallback authentication used in password resets. Most importantly, this research provides solid foundations for the design and analysis of future authentication systems based on implicitly learnt information.

For indirect implicit learning-based authentication secrets, I propose a mechanism for training users on system-assigned passphrases using the concept of contextual cueing along with semantic priming, intended to offer resistance to online guessing attacks. My proposed approach improves the usability of this type of authentication secret by taking advantage of implicit learning techniques.

In an 880-participant online study, I explore the feasibility of my proposed approach. The results showed that the proposed approach improves usability of system-assigned passphrases, both in terms of recall rates and login time. The results of my study showed 88.61% of authentication success rate one week later for the participants who received the implicit reinforcement training.

		Success first attempt	More attempts	Avg login	Total success
Conditions	Implicit Training	83.54%	5.06%	13.74	88.61%
	Control	51.39%	5.56%	45.78	56.94%

Table 1.1 Third login session total success rate percentages, the percentages of those who needed more attempts to login, and average login duration (in seconds) for each condition.

1.3 Thesis Statement

Following the above introduction, the main thesis which runs throughout and motivates my work is summarized as follows:

Implicit learning has many properties that may prove useful in authentication systems. I hypothesize that implicit learning can be used directly for secure authentication and indirectly for improving the memorability of system-assigned authentication secrets. This motivates the following research questions:

Question 1: Can users' implicit memory be employed in order to assign them the configurations of a random set of CC displays as a random password, and evaluate the acquired knowledge later on?

Question 2: Can users be authenticated on their implicitly learnt CC knowledge based on one measure; that is, reaction time?

Question 3: Can the performance of the approach be further improved by having more distinctive information to measure the implicitly learnt information using users' eye movements patterns?

Question 4: Can IL improve memorability of system-assigned passphrases?

Question 5: Can the power of the contextual cueing effect be harnessed indirectly along with the semantic priming effect to make system-assigned passphrases more memorable?

Question 6: Are improvements using IL-based interfaces due to repetitions or time exposure in the training phase and recognition in the login phase?

Question 7: Is the effectiveness of the reinforcement approach due to recognition during login, or our special IL-based training?

Question 8: Given the effectiveness of the training provided with the combination of CC and SP for passphrase memorability, can we improve security of the proposed passphrase scheme by not exposing any cues for the login session?

1.4 Research Contributions

This thesis proposes new authentication approaches based on direct and indirect use of implicit learning. This endeavor is novel through the following contributions to the field of security:

- *A novel authentication approach, called Tacit Secrets, design and implementation.* Using a direct implicit learning mechanism, I performed the design and feasibility study of a method for producing Tacit Secrets, which the user can remember, despite the fact they cannot write them down. My positive feasibility study results demonstrate that implicit learning can be used to produce a user authentication system with high accuracy, and strong security properties, and as such might be employed in future authentication systems research.

- *Tacit Secrets security analysis.* I perform analysis to quantify the scheme's security against multiple attacks. For Tacit Secrets, I first analyze the proposed scheme false positive rate. I then carry out additional security analyses to determine Tacit Secrets's resistance to attacks based on observation, classical phishing, and online attacks using population statistics.

- *Comparison of Tacit Secrets with previously proposed methods.* I compare the scheme with two previously proposed implicit memory-based methods [31] and [2]. The result shows substantial improvement in authentication duration, training time, and success rate.

- *Incorporating ocular parameters into Tacit Secrets.* I incorporate two ocular parameters to improve the performance of the approach.

- *Evaluating different configurations of Tacit Secrets.* In order to make the scheme more usable by offering shorter login time, I assess the approach by simulating different combinations of display numbers to find the optimum number of displays for an authentication session.

- *A novel authentication approach, called Implicitly Reinforced Passphrases and its design and implementation for system-assigned passphrases.* I propose *Implicitly Reinforced Passphrases*, a novel authentication approach to reinforce system-assigned passphrases through implicit learning techniques. I design, implement, and test instances of the approach that offer resistance to online attacks, have short training times, and reduce passphrase login errors.

- *A demonstration of the efficacy on Implicitly Reinforced Passphrases.* I analyze the feasibility of the proposed approach using data collected through a 880-participant online study on Amazon Mechanical Turk. My analysis indicates that the approach significantly improves the memorability of system-assigned passphrases and the login times. The result suggests the improvement is due to the IL approaches rather than recognition, exposure time, or repetition.

1.5 Organization of Thesis

The remainder of this thesis is organized as follows:

- **Chapter 2** provides an overview of human information processing, cognitive abilities, implicit learning, contextual cueing, and semantic priming.
- **Chapter 3** provides a literature review related to authentication in general and the shortcomings of text-based passwords. I then continue by describing related works on authentication under duress and passphrases. The chapter finishes by providing some details on the methodologies used in this thesis.
- **Chapter 4** proposes system-assigned authentication secrets that use implicit learning directly, "Tacit Secrets". The design, implementation, user study, results, and security analysis are discussed in this chapter.
- **Chapter 5** proposes authentication secrets that rely on implicit learning indirectly in the sense it is used to reinforce explicit memory rather than test implicit learning directly. It describes the design, implementation, user study, and results for this approach of, "Implicitly Reinforced Passphrases".
- **Chapter 6** provides more discussion related to the two proposed approaches.
- **Chapter 7** discusses the summary of the results and offers concluding remarks and future directions.

Chapter 2

Background

This thesis is primarily focusing on an implicitly-learnt knowledge-based authentication scheme using the contextual cueing paradigm. By providing an implicit mechanism of learning, users are trained on a secret, and the secret is then used for authentication purposes. This chapter is used to describe some of the different topics that form the foundation of this thesis. Accordingly, I first provide an overview of human cognitive abilities and information processing. I then provide related works on implicit learning and explain more about the applied cognitive paradigm; that is, *contextual cueing*, which I am using in the designed approach.

As per indirect implicit learning-based authentication secrets, I use the *contextual cueing* paradigm along with another paradigm, called *semantic priming* to enhance memorability of system-assigned passphrases. Hence, I provide background and review of other studies regarding the semantic priming paradigm.

2.1 An Overview of Human Cognitive Abilities

Generally, a *process* refers to any series of actions whereby something is operated on, in order to produce some results. A *cognitive process* is a mechanism by means of which an individual's mental contents are operated on to generate some responses. These mental contents are formed by different encodings and representations which an individual makes from external stimuli, knowledge, rules, scenes, images, and identical content originating from either short-term or long-term memory. The responses can be either observable (overt) or unobservable (covert) [32].

Cognitive skills are revealed by those types of tasks requiring many actions to be correctly chosen and conducted. These skills can be classified into two different groups containing procedural skills, which the sequence of actions matters, and non-procedural cognitive skills, which only finite state matters [33].

2.2 An Overview of Human Information Processing

Human beings have two main control modes, including controlled or conscious processing, and automatic or unconscious processing. Cognitive activities are directed by a complex interaction of these two modes. Controlled processing is related to the attentional mode in which information is processed by working memory. The attentional mode is effortful, slow, and sequential.

Cognitive Load Theory [34], which proposes designing learning material based upon human cognitive architecture, results in effective learning. Such an architecture consists of a working memory, which is limited in terms of the capacity and the span when it is employed for novel information processing. On the other hand, there is long-term memory with unlimited capacity. The capacity and the duration limitation of working memory for processing of the new information are bottlenecks. In other words, a limited amount of information elements can be kept in working memory. In addition, this amount decreases when an individual needs to remember some information and then process it. This process is required due to some interrelation of information elements and the need for merging them. Nonetheless, information which has been previously stored in long-term memory, namely cognitive schemata, is considered as a single information element in working memory. As a result, prior knowledge or skills about a specific task can decrease the cognitive load for that task, leaving more capacity of memory for other information and processes.

According to the cognitive memory model proposed by Atkinson and Shiffrin [35], they suggest the multi-store structure of human memory containing three different memory stages, including sensory, short-term, and long-term memory wherein information flows throughout (see Figure 2.1). They treat information processing as a linear process where information flows from sensory memory through short-term memory and finally into long-term memory. Once information is detected from the environment, it is temporarily stored into sensory memory. The information retained in this memory has a very short lifetime (1/4 to 1/2 second) and it decays rapidly. Short-term memory, which is also called working memory, relates to what we are thinking about at any given moment in time. The duration of this memory is longer than sensory memory (15 to 20 seconds). However, long-term memory is with unlimited duration and capacity; that is, it can last anywhere from a few days to a lifetime. If information is sufficiently well rehearsed, it is able to pass into long-term memory.

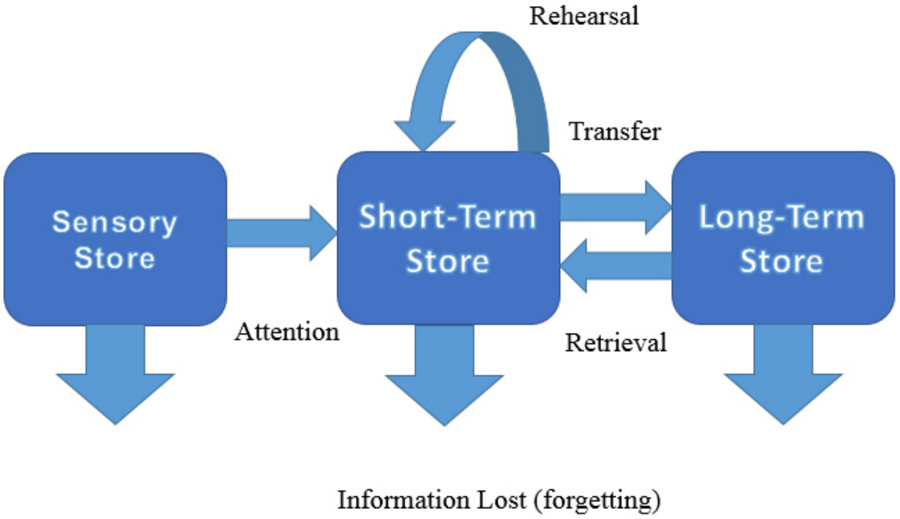


Fig. 2.1 Multi-store model of memory (Atkinson & Shiffrin, 1968)

For any authentication secret to be memorized is the ability to sufficiently retain the authentication credentials in short-term (working) memory in order to be transfered to long-term memory [36, 35]. This is the key factor which needs to be deemed during the memorization process.

2.3 Implicit Learning and Contextual Cueing

Implicit learning (IL) is a fundamental and ubiquitous process in cognition. IL is natural capability by which we can acquire skills throughout the course of repetition of specific tasks. Such skills are acquired unconsciously, unintentionally, and without having declarative knowledge about what has been learnt [25, 37, 38]. IL is associated with complex features or probabilistic patterns, whereas explicit learning is most probable when stimuli are salient [39].

Implicit and explicit learning can be distinguished by the degree of conscious or deliberate processes by which underlying complex structure is discovered. IL involves a part of the brain called the basal ganglia that learns tasks by repeatedly performing them. This implicit mechanism of learning is used in different areas such as perceptual-motor skills, language acquisition, social intuition, or detecting a target in a complex scene. [37]. Such a learning involves associative learning mechanisms which employs statistical relations in the environment in order to create highly specific knowledge representation.

To investigate the hypotheses related to human implicit learning, different paradigmatic methods are used. In 1967 Reber [40] first studied artificial grammar learning. The artificial grammar learning paradigm [41] is another method employing to explain about IL. This experiment is followed by using a finite-state grammar which makes some strings of letters. During a training phase users are shown sequences of letters which are either rule-based (grammatical) or random (non-grammatical) sequences. Through a testing phase, they should then distinguish between these two kinds of sequences. They perform this task with better-than-chance accuracy, while they do not realize any existing rule. In both aforementioned experiments, participants are unaware of the existing rules and repetitions. They are provided with some instructions about individual items which prevents them from focusing on the overall material structure. Indeed, an important feature of IL is the incidental nature of acquisition process.

Serial Response Time (SRT) task [42] is another study toward IL through which users respond to a visual-motor procedural learning task. Through this task, a fixed set of visual stimuli is displayed in one of four positions arranged horizontally on a computer screen. Given specific instructions, subjects are asked to pres as quickly as possible a corresponding button for each position. The users' search performance improves over time and repetition on previously seen configurations compared with novel displays. Incidental learning of the sequence happens without the need for explicit knowledge or awareness.

The main strategy to set up an experiment regarding IL is adding a secondary task following the training phase, and then assessing participants' performance. IL experiments are usually followed by some post-experimental tasks, namely recognition tests, which explore participants' explicit knowledge.

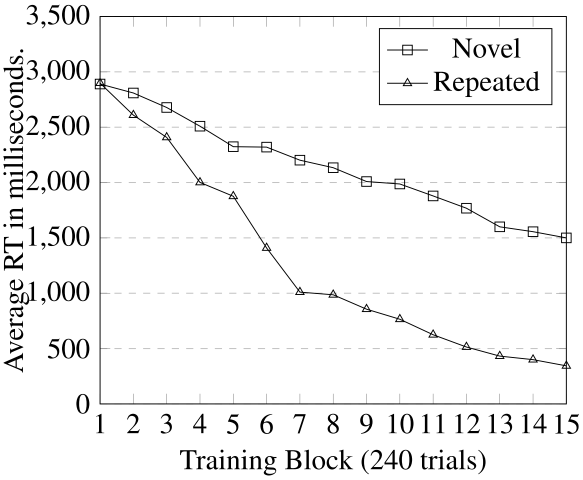
In effect, visual search is an inseparable part of everyday life. Visual context, such as the spatial configuration of objects, guides human attention to a target location [43, 44]. To allow memory and knowledge collaborate in order to handle visual search, humans usually build and structure environment precisely. Biederman [43] found visual context, such as the spatial configuration of objects, guides human attention to a target location. For example, we may need to identify a traffic signal amongst an array of information in a busy street. Such a search might be facilitated by repeatedly seeing that the location of traffic signals are most often to the right of street signs. Repeated exposure to such patterns allows implicit learning of these probabilities, which in turn facilitates quick guidance of our attention towards the most likely target location.

Contextual information is an important stimulus guiding attention and specifies which object should appear in a scene and where. Objects and events occur in a rich visual context, helping their recognition. This context tends to be predictable, because one's visual experience is not based on a random sample of objects; it is structured and repetitive. The role of context is to provide a match between the incoming perceptual inputs with constant context knowledge acquired through past visual experiences. Chun and Jiang [45] first developed a new paradigm called Contextual Cueing (CC) to study implicit learning and memory using a specific perceptual task. CC is a mechanism [45] through which visual attention can be guided by implicitly learnt knowledge [46]. CC is a robust effect that persists after delays lasting six weeks [29, 30]. It also vigorously resists retrospective interference [47, 29]; that is, the CC effect diminishes when the target, and only the target, is re-positioned elsewhere in an old display. Zellin et al. [29] suggest that relocating the target necessitates extensive training for the subjects to make them permanently adapt their previously acquired knowledge of the context to the relocated target context. Merrill et al. [18] suggest that CC is independent of IQ since persons with intellectual disability (i.e., Down syndrome, Fragile X syndrome, and unknown etiology) also exhibit contextual cueing effects. The capability of CC to remain intact in several neurological and mental disorders makes that more fascinating. For instance, CC survives unbroken in autistic spectrum disorder (ASD) [48], dyslexia [19, 20], Korsarkoff's syndrome [44], and schizophrenia [49].

A context can be defined as a 2-dimensional spatial configuration of irrelevant (distractors or non-target) objects in which a target is presented. In effect, CC relies on the distractors providing spatial cues to the location of a target. The entire context is embedded into a display. To investigate CC effects in the laboratory, subjects are typically asked to search in a display of objects to find a target. If a target is shown in a *repeated display*, i.e., a display that repeats throughout a training session, subjects' performance in finding the target increases [38, 50, 51]. Chun and Jiang [51] found that the difference of reaction time between previously unseen (*novel displays*) and seen (*repeated displays*) was significantly different.

Reaction time (RT) refers to the time it takes a participant to find the target, which is presented through a visual search task. See Figure 2.2 for this effect on my experiment described in Section 4.7).

Fig. 2.2 Search RTs as a function of display type (novel and repeated) and block in the training session of the experiment described in Section 5, showing the difference in response time between repeated and novel displays.



Such contextual knowledge is acquired through IL processes which facilitate acquiring the complex information about the stimulus environment without intention, consciousness, and awareness [25, 37, 38]. Chun and Jiang [51] showed the participants were typically unable to explicitly recognize such predictive contexts through a post-experimental classification task. Such incidentally acquired contextual knowledge makes an instance-based, highly robust, and durable implicit memory for context [51]. Chun and Jiang [51] also found implicit memory for spatial contexts are robust and durable over time, lasting for days, weeks, even months (e.g., 6 weeks [30]) in both normal observers and even patients with amnesia. For these reasons, it seems that contextual cueing may offer some unique advantages in authentication systems.

There are also some previous works showing that how other contributing factors can affect the efficiency of visual search. For instance, Duncan et al. and Pomplun investigated how the existence of more similarity between the target and the distractors, can make the search task more difficult [52, 53]. This similarity has been applied in the typical CC task by choosing '*T*' as target and '*L*' as distractors.

2.4 Semantic Priming

For indirect implicit learning-based authentication secrets, I aimed to further explore how the effect of contextual cueing alongside a psychological phenomenon, called semantic priming, can be used to enhance user's memorability of system-assigned passphrases. The idea is to use contextual cueing and semantic priming paradigms to leverage implicit learning in order to aid the memorability of secure system-assigned passphrases. Thus, in this section I explain more about the semantic priming effect and related works conducted in this area.

Semantic memory is often described as humans' acquired, structured record of facts, meanings, concepts, word naming, lexical decisions, generic knowledge about the external world, and semantic priming [54]. The research around this type of memory has been drastically influential in the science of memory and word recognition. On the other hand, priming is an improvement of performance in a cognitive or perceptual task, relative to an appropriate fact, produced by context or previous experience [55]. The phenomenon of semantic priming turns out to be as a result of the connection between semantic memory and priming effect. It has captured the attention of several decade of research of cognitive scientists. Various psycholinguistics researches have studied semantic priming. Essentially, semantic priming is a rich source of information about the mental lexicon which is driven from meaning relations between lexical items. In semantic priming, a target word (such as dog) is preceded by a semantically related prime word (such as cat), it is processed more quickly and efficiently than when preceded by an unrelated prime (such as book) [55–57]. In 1971, one of the most influential research in cognitive psychology was published by Schvaneveldt and Meyer [58]. They had their subjects deciding whether two strings of letters (i.e., word-word) are both words or not. When the words are semantically related the average response time are 85 milliseconds faster compared to unrelated pairs. Semantic priming results in the improvement in speed and accuracy to respond to a stimulus (e.g., word, picture). For many years of research semantic priming paradigm has been used as a tool to improve understanding the organization of the mental lexicon and word retrieval from long-term memory [58].

In the classical and early demonstrations of semantic priming experiments, two simple verbal tasks are defined; Lexical Decision Task (LDT) and naming tasks. Through a typical LDT experiment, each trial contains a display including a target and prime. Participants are instructed to read the word silently and decide whether the target word is a word or non-word. The stimuli consist of correctly spelled words and meaningless strings of letters called "non-words" (e.g., smti). Through each experiment trial, participants are provided with a target and a prime word. They are asked to read the prime silently and decide on the target word as being a word or a non-word. The findings of these studies confirm the higher accuracy and decreased latency in decision making are achieved for the semantically related target and prime compared to unrelated pairs [55]. Another common experiment related to semantic priming is naming or pronunciation task. In this experiment subjects are asked to read target words aloud as quickly as possible. The same finding is implied such that when the target word is accompanied by a semantically related prime, subjects have faster reaction time and more accurate responses.

Chapter 3

Related Works

As discussed in Chapter 2, the focus of this thesis is on system-assigned knowledge-based authentication approaches, enabled by implicit learning. Given the provided background on the cognitive paradigms used on this thesis, in this chapter I first provide related works on the proposed implicit-based authentication. I then discuss system-assigned authentication secrets as both of the proposed schemes are system-assigned secrets. Since I claim the proposed approach is resistant to some coercion attacks, I discuss some related works which are claimed to be resistant against coercion attacks. As per our indirect implicit learning-based authentication secrets approach, I am focusing on system-assigned passphrases which users are trained for through our special training mechanism. Thus, I also discuss related works on passphrases in this chapter.

3.1 Introduction

The popular use of passwords that people choose is controversial—people tend to choose the same or similar passwords across multiple accounts, many of which have been leaked in password breaches. The wealth of password data that is publicly available has been shown to enable targeted guessing attacks that successfully guess over 32-73% of passwords within 100 attempts [10]. This motivates other approaches to user authentication.

Over many years of research, several authentication methods are proposed as substitutes for text-based passwords due to several well-known shortcomings of this traditional and at the same time the most popular authentication scheme. In effect, each authentication method has its own strengths and weaknesses in terms of security, usability and deploy-ability. Nonetheless, based on the nature of the environment that they are provided for, these factors can be compromised. Despite the variety of proposed mechanisms, text-based passwords persistently survive and are used by most developers and users. Researchers [59, 3] contend that, it is unlikely for text-based passwords to be replaced by substitutes in the near future.

Indeed, widespread usage and relatively low implementation cost of knowledge-based schemes such as passwords are the main reasons for their prevalence and tenacity; moreover, continuous failures of substitutes for web authentication dampens any radical change. Thus, knowledge-based authentication schemes may well become even more popular as users need more accounts for their daily tasks or some accounts with high-security requirements. For these reasons, I look for ways to improve knowledge-based authentication schemes to make them more usable and secure with less sacrifice of one for the other.

In striving for usable security and including human factors as part of system design is an important consideration that has a direct impact on the security of the system. Giving users free rein to choose their authentication keys, users tend to select much simpler passwords to remember which are also easy to guess while randomly-generated system-assigned secrets provide more security. Nevertheless, due to the difficulties with regard to memorizing system-assigned secrets [60], they are plagued with usability problems which preclude users from using them, making them ineffective [61]. System-assigned secrets do not make any meaningful connection with the user [62]. Since the user has not had any cognitive involvement in the creation process. Thus, the proposed schemes for improving knowledge-based secrets have yet to deliver the desired security and usability gains.

For direct implicit learning-based authentication secrets, I investigated how users' learning process can be aided using an implicit learning mechanism. Although the designed approach resulted in an acceptable success rate for authentication, the whole training and authentication process is longer than traditional authentication schemes. The long duration can make using such a scheme difficult for daily authentication purposes which they do not need high level of security.

I also propose and evaluate another approach, I call *Implicitly Reinforced Passphrases* to improve memorability for system-assigned passphrases using implicit memory techniques. The essence of the idea is to reinforce the passphrase using a short implicit learning (IL) phase during enrollment, in order to involve both implicit and explicit memory processes. IL occurs through the repetition of a specific task. Implicitly learnt skills are acquired unconsciously, unintentionally, and without declarative knowledge about what has been learnt [25, 37, 38]. IL is associated with complex features or probabilistic patterns, whereas explicit learning is most probable when when involving salient stimuli [39]. Implicit learning is used in different areas such as perceptual-motor skills, language acquisition, social intuition, or detecting a target in a complex scene [37].

I design and implement an instance of *Implicitly Reinforced Passphrases* using 4-word passphrases, intended to offer resistance to online guessing attacks, phishing attacks, and leaks from other verifiers. Our design employs two IL techniques: contextual cueing and semantic priming, both alone and in combination. The system design also aims to reduce input errors and long login times associated with other passphrase systems [63–65].

I evaluate our system through a 880-participant online study involving five control conditions that allow us to identify which, if any, IL technique produces the best result. The results demonstrate that our design offers significant memory improvements, with short mean training and login times (1.33 min and 13.74 sec, accordingly). My results also suggest that the improvement can be attributed to the employed implicit learning techniques, as opposed to repetition or recognition. Although repetition is a component for IL, when it is used by its own, it dose not provide memorability benefits. a Participants reported high levels of satisfaction with the scheme and 77% preferred to use it in real life as a replacement to traditional textual passwords.

3.2 User Authentication

Electronic authentication is an integral part of computer security and involves an electronic process of confirming users' identities when access an information system. This process acts as an access control, seeking to confirm a user's authenticity to grant access to different accounts. Technical challenges are emerged when this process is conducted through a remote connection of individuals [66]. Depending on what type of information is used for authentication, this information falls into different categories, including something the user knows (knowledge-based), something the user has (token-based [67]), something the user does (behavioral), something the user is (biometrics [68]), and someone the user knows [69]. Providing enough proof in one or some of the mentioned categories results in verifying what the user claims be to. All these categories have their own advantages and disadvantages [70].

Alphanumeric password is the de facto standard of authentication. For many years of research, a plethora of authentication schemes have been proposed, derived by the promise of improved password memorability, usability and at the same time strong security. Furthermore, to come up with some of the existing weaknesses of the proposed replacement schemes, pairs of solution are also combined in order to play complementary roles. Hence, there has been a continuous concern for information systems developers to verify a claimant's identity using the most secure and usable authentication protocols. However, despite the large number of alternatives for authentication, text-based passwords stubbornly remain to be the basic and the most relied-upon security mechanism since they are simple and inexpensive to implement, familiar to the users, no physical burden, and no need to use people's private biometric data.

In this work, I particularly focus on "something user knows" and introduce a new approach using the concept of implicit learning. Generally, humans' knowledge can be categorized into two main types, “conscious knowledge” (e.g., passwords) and “subconscious knowledge” (e.g., implicitly acquired knowledge). Much of the information we acquire from our external environment involves processes that do not require conscious awareness [25]. Implicit learning happens as a result of internalizing the regularities that take place in the external environment. We are surrounded with several regularities and patterns in our everyday life. This knowledge acquisition that occurs through processes without conscious awareness has been termed *implicit* [25]. Such knowledge has been put forward as a fundamental process in allowing acquisition of complex information [26, 27]. We take advantage of these attributes to present an authentication scheme that not only decreases the burden of recalling credentials on the user but also it can be resistant against coercion attacks in which the user is forcibly asked to reveal credentials.

This section is organized as follows: Relevant background on the area of implicit authentication is discussed in Section 3.2.1. System-assigned secrets and passphrases are explained in Section and 3.2.2 accordingly. As implicit learning based authentication keys provide resistance against coercion attacks, in Section 3.2.4, we review some of the proposed techniques used to resist coercion attacks.

3.2.1 Implicit Authentication

Authentication as a process of identity verification has gained substantial importance in modern and developed societies. Users need to access multiple systems and accounts and granting proper access with high true positive and low false positive rates is a challenge of many systems. Over the past few years, cyber security has become the main target for the attackers and several gigantic breaches have occurred commonly. On a regular basis, we learn of new attacks harming individuals and organizations. These attacks are performed through different ways such as brute-force attacks, shoulder surfing, social engineering, malware, key logging, etc. These have been detrimental for both individuals and businesses by compromising valuable and sensitive data that is digitally stored. Therefor, in light of the importance of human factor in the security chain, having more human-centered approach is absolutely vital. Security solutions will fail if users perception is not taken into account. Users' willingness is the key factor to admit any security policy and it cannot be achieved unless users perceive a policy easy-to-use.

Current authentication methods can be divided into three main areas, including token-based, biometric-based, and knowledge-based authentication. Several alternatives on each category have been proposed to tackle different issues related to the security and usability of the existing authentication methods. All aiming to alleviate the burden of memorization with acceptable security level. The proposed solutions were looking for secure and usable authentication; however, finding a balance between these two important attributes is difficult and the majority of the previous works compromise one for another. Thus, none of the proposed alternatives has proven sufficiently enticing making passwords to remain as the de facto method of authentication for many systems.

One recent trend is using knowledge based authentication where implicit memory is involved in memorization of the authentication secrets. Several implicit authentication methods have been proposed using users' patterns of interacting with a system. Note that these methods do not use implicitly learnt information in the authentication process; rather, they can be considered a form of behavioral biometric. Babu et al. [71] propose the Transaction-Based Authentication Scheme (TBAS) for Personalized Multimedia. To distinguish a genuine user from the attacker, the proposed model logs actions or reactions of a client while formulating and executing transactions, transaction time behaviors, and a summary of various suspicion factors of the observed user's transactions. All these cognitive measures can facilitate identification of an attacker. Such mechanisms can be replayed if the attacker coerces the user to interact with the system as he/she does every day. These types of authentication are specifically useful for continuous authentication and are vulnerable to coercion attack. While Tacit Secrets cannot be replayed, it might be vulnerable when the adversary uses physical force such as wielding a gun, and threatens the user's life to coerce the user to login via Tacit Secrets. To prevent such cases, the system for which Tacit Secrets is used could be equipped with a video surveillance system which can capture and detect such situations. DeLuca et al. [72] note that current password patterns for Android devices are usable and memorable; however, in terms of security, they are weak since the shapes (e.g., Draw-A-Secret [73]) are easily stolen or reproduced. They propose an implicit authentication method for touch screen smart phones which uses an additional security layer that makes their system more secure. Their proposed approach authenticates the users not only by the shape but also by how they interact with the device using a sequence of time series of touch screen data.

Bojinov et. al [31] proposed an authentication scheme based on the use of implicitly learnt information [31]; however, this approach had very low success rates and high times for training and login. My work is related to that of Bojinov et al. [31], who designed an authentication scheme using implicit learning with the goal of thwarting coercion attacks. The scheme of Bojinov et al. [31] offers the property that users are unaware of their secret and thus incapable of leaking it to an attacker who does not know the correct secret. Their scheme used the Serial Interception Sequence Learning (SISL) task originally introduced by Sanchez et al. [74]. Subjects were trained to implicitly learn a random key sequence using a game similar to the Guitar Hero video game. After a 30 to 45 minute training period, they were tested through a session of playing the same game. Figure 3.1 indicates a sample training task for the users in their study.

The authentication process in this scheme is based on the users' performance (the percentage of the correct responses and response time) on the learnt sequence versus random ones. This data can be used to prevent coercion attacks; however, only 71%, 47%, and 62% of participants could successfully authenticate using this method immediately, 1 week, and 2 weeks later, respectively. Our study of Tacit Secrets included an immediate, 2 days, and one week later testing sessions which resulted in 100%, 96.15%, and 92.86% authentication success rates, respectively. These results are quite promising in comparison with the SISL

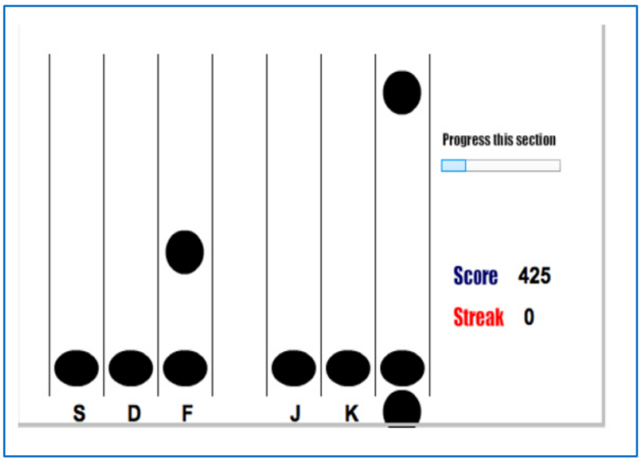


Fig. 3.1 Screenshot of SISL task (from [1]).

task [31]. Their first experiment aimed to confirm the existence of implicit learning through an authentication session immediately after training; Their second experiment had two groups of participants: the first group did the SISL task one week after training. The second group did the SISL task two weeks after training, where the length of the testing session was doubled (from 5-6 minutes to 10-12 minutes) to see if this change could affect their performance. For this second group of participants, 61% exhibited better performance on the trained sequences.

In another study, Denning et al. [75] proposed an authentication scenario which employs a priming effect as a mechanism using implicit memory. Their suggested image-based authentication system used pairs of images; that is, complete and degraded counterpart images. They initially showed sets of complete images and for later authentication, degraded images are exposed through a familiarization task. Since the scheme involves the conscious learning of the images, it does not provide any resistance to the coercion attack. Furthermore, the requirement to provide a large set of images makes the system less attractive for developers to implement this authentication mechanism for their systems.

There are also several visual features that allow us to accurately distinguish users based on differences. While some of the previous works focus on detecting individual differences using these measures, I stress that I only use them for detecting implicitly learnt keys. Ebrez et al. [76] discuss how human eye movement patterns can work as discriminative factors for authentication. Their known features are categorized in three main groups, including pupil, temporal, and spatial features. They test these features on a set of general tasks. Although there is a visual search task and not a group of different tasks in my study, I can still take advantage of some of these features such as static pupil feature, and other temporal and spatial features related to the user's saccades and fixations while doing the task.

Recently, Castelluccia et al. [2] proposed MooneyAuth, a scheme that also employs implicit memory to reduce the cognitive burden of recalling traditional passwords. During enrollment, users are provided with Mooney images that work as primes, along with the corresponding original images and their labels. Mooney images are degraded two-tone images of an object. This object is usually difficult to recognize at first look; however, during enrollment, users learn the association between these images and their labels. After training, users outperformed labeling these previously seen Mooney images over other images during the authentication phase. A long-term study revealed substantial improvements for MooneyAuth compared to a previous implicit-learning based authentication scheme [75], demonstrating its potential for fallback authentication. MooneyAuth has an average authentication time of 3.5 minutes, 0.1% FAR, and 97.14% TAR. Although the scheme offers performance improvements over comparable previous work [75], it does not provide resilience against a number of attacks that the Tacit Secrets approach does (e.g., observation, classical phishing, guessing, and coercion attacks). Additionally, the Tacit Secrets approach recommended configuration has shorter login times. Figure 3.2 indicates an example fo a Mooney image.

3.2.2 Passphrases

Tex-based passwords are the most commonly used authentication in many of today's systems. To enhance security, users are advised to choose longer passwords which contain

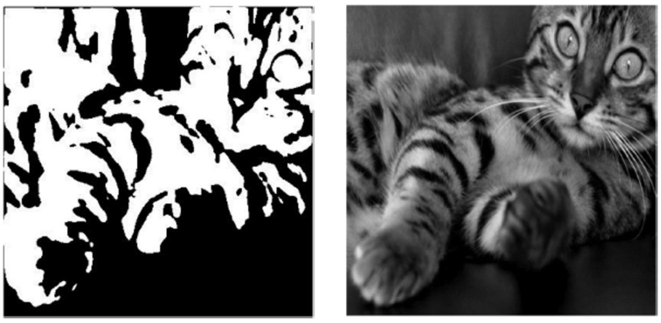


Fig. 3.2 An example of Mooney image (from [2]).

more characters of different categories (i.e, letters, digits, symbols). Due to the increasing number of accounts users need to access, using complex passwords, it is highly likely to forget them. To avoid problem of reseting passwords when forgotten, users have high tendency to reuse, write down, insecure storing, or use predictable patterns and words for their passwords [77]. All these behaviours are undesirable and should be prevented to enhance security.

Passphrase authentication is an extension of the traditional password authentication. Passphrases are long passwords created from multiple words to form a phrase, e.g., “I love reading books”. Passphrases, space-delimited sequence of natural language words, are one of the knowledge-based authentication tools whereby a single password is substituted with a phrase which can be a sentence in a natural language. The idea of using passphrases turns back to 1982 when Porter [78] offered it; however, most of the systems have length constraints for the passwords (e.g., 8 characters) which makes the use of passphrases infeasible. Passphrase offered aiming to improve security by hardening brute-force attacks in addition to simplifying memorability. Human memory limitations are one of the most important issues for usability of knowledge-based authentication keys.

This tool turns out to be just as memorable as passwords [79] or more memorable than passwords when it follows a sentence structure [60]; however, users tend to select a phrase that means something personal. Bonneau et al. [80] studied the linguistic properties of Amazon Payphrase of 100,0000 users. They found out using lists of popular books and movies, as well as bigrams taken from an existing natural language corpus, will simplify guessing these phrases hereby increases guessing attacks success rate. Passphrases can also increase the accuracy of behavioral biometrics such as keystroke dynamics when same data is inputed by different individuals.

Since passphrases are subject to a high rate of typographical errors and user dissatisfaction [79]. When users type a word, it usually involves different stages, including automatic recognition of words, translation of words into keystrokes, and execution of keystrokes [81]. Typing errors may occur within each stage; however, keystrokes have higher potential in making errors. Some studies have been proposed mechanisms to lower these errors. Previous works suggest detection and correction of spelling errors and storing multiple hashes of a passphrase to find the closest match [82, 83]. Other probing approaches propose using real time visual feedback to advice users while making typos [84].

Since passphrases consist of a sentence or a phrase, they can benefit by using mnemonics [85]. Memorization is a difficult part of any learning mechanism; however, this labourious process can be facilitated by a learning technique, called mnemonic keywords [86]. This memory aid can be used in different ways such as an abbreviation, rhyme, or mental image that helps to recollect something. This technique can simply applied to any task that needs memorization. Previous studies have investigated the improvement in memorization and pronunciation of foreign languages vocabularies using keyword associations [87–89].

Shay et al. [90] conducted an online study via Mechanical Turk to delve into system-assigned password and passphrase composition policies. They considered eight different passphrase conditions and three password conditions. Participants in their study were not instructed to follow any particular mnemonic techniques. They found no significant difference in memorability of system-assigned passwords compared to system-assigned passphrases of equivalent password strength.

3.2.3 System-Assigned Secrets

Humans have limited ability in recalling unrelated sequence of words. The span of human memory imposes noticeable limitations on the amount of information that can be received, processed and recalled [91, 92]. Users rarely choose passwords that are both hard to guess and easy to remember. While using system-assigned passwords was a common practice in the middle of 80s [93], it did not last for the 90s since the NIST standards assume the user's choice for passwords [66]. It is worth noting that today's systems and technologies also play an important role in weakening human's ability to recall keys as they provide mechanisms for users to rely more on their devices than their memories.

Although passwords complexity policies were initially offered to encourage users for strong passwords, they are more effective for augmenting the entropy [94, 95] while advance attackers are still able to efficiently crack such passwords offline. On the other hand, randomly generated secrets provide more entropy and they are more resistant against offline attacks but suffer from memorability issues. Such keys demand an increased cognitive load which makes end-user taking insecure behavior such as share, reuse, or writing down the assigned key. The low memorability is due to the fact that humans are more prone to forget random information which they do not have any past experience or relation with them. Thus, due to low adoption rate as well as usability issues related to this type of secrets [79, 96], they are commonly used for highly privileged accounts such as critical system configuration terminal, high-security vault or room, or encrypted files.

Researchers have proposed different schemes to overcome the existing issues related to system-assigned secrets. Jeyaraman and Topkara [97] propose random generation of a lower-case password and creating a mnemonic for the randomly generated password to make it easier for recall. Crawford et. al [98] also offer using pronounceable text for creation of random secrets. Al-Ameen et. al [99] try to find an ideal middle-ground between security and usability. They suggest using a scheme called Cued-Recognition (CuedR) which combines various memory cues, including graphical, verbal, and spatial cues for system assigned passwords in order to facilitate a detailed encoding of these authentication keys on users' memories. This encoding results in the authentication information to be transferred from the working memory to the long-term memory. It ultimately helps users to recognize their images when logging in later. In the lab study with 37 participants, they found 100% of successful recall one week after registration.

I aim to provide usability for a type of knowledge-based system-assigned secrets; known as, passphrases. Shay et al. [100] found no significant difference in memorability of system-assigned passwords compared to system-assigned passphrases of equivalent password strength. This suggests that system-assigned passphrases may also place a burden on users' memory unless the suggested approach provides some form of memory aid and increases users' satisfaction level. According to the findings of Shay et al.'s study, there is no remarkable difference in the memorability and users' satisfaction of a 3-word passphrase compared to 4-word. On the other hand, due to the higher entropy of 4-word passphrase compared to 3-word, I decided to make the passphrases contain 4 words. 2-word passphrase does not provide enough security and increasing to 6-word passphrase users can cause usability issues by increasing the training as well as the login time. Thus, the goal was to take advantage of the CC effect and semantic priming to make system-assigned passphrase more usable.

One commonly recommended approach is the use of passphrases [101]. Based on the NIST definition: "A passphrase is a collection of words (typically more than 20 characters), that is used to authenticate the identity of a computer system user and/or to authorize access to system resources [102]". Passphrases as a collection of words used instead of a password, intended to increase password length and therefore security, while retaining memorability [63]. Passphrases are more memorable than passwords when they contain meaningful expressions or follow a sentence/gramatical structure [63, 103–106]; therein lies the security drawback. Bonneau and Shutova [107] studied the linguistic properties of Amazon Payphrases for 100,000 people. They found that if an adversary were to use lists of popular books and movies, plus natural language bigrams, they could successfully guess many of these phrases [107, 108].

To combat the security issue, system-assigned passphrases was proposed, but this comes at a cost to memorability. It has been suggested that if people pair a system-assigned passphrase with a story, it would improve memorability [109]; however, studies indicate that this is not a successful strategy [64]. This motivates other approaches to improve the memorability of system-assigned passwords. The use of spaced repetition has been used to improve passphrase memorability, but at the cost of a long training time [65]. Using multiple verbal and graphical cues has also yeilded memorability improvements, but the login times remain long [110].

3.2.4 Authentication Under Duress

Coercion resistance is one of the most important and intricate security requirements for some systems. A coercion attack is when the key holder is threatened or extorted to reveal their key (e.g. the password to an encrypted file), to make the system accessible for the attacker. This attack can be quite effective and may also threaten the user's life, but is seldom considered in proposed authentication schemes. For instance, biometrics contain distinguishing features that can recognize an authentic user from an imposter; however, not all of these these methods are resistant to coercion attacks as an adversary may force the user to provide their biometric data.

Many knowledge-based authentication mechanisms such as passwords and token-based mechanisms are also vulnerable to coercion attacks. Implicit learning allows us to learn users a key that they are unable to state or reveal, even if coerced.

Here a few related works proposed to resist against coercion attacks are highlighted. Clark and Hengartner introduced panic passwords [111], where any user has a regular password and another, panic, password. The panic password is used to indicate a duress situation to the server. The main goal is protecting both user and information secrecy;

however, it can lead to more load for the user to memorize both passwords while they can be easily forgotten, especially in a stressful situation. Moreover, by mistyping the passwords accidentally, it can lead to many false alarms. Gupta et al. [112] use biometrics to resist coercion attacks in generating cryptographic keys. They use voice [113] and skin conductance [112] measurements to provide a key generation mechanism resistance while the user is under duress. They showed this measure can reveal the user's emotional states and recognize if he/she is under the attacker's control; however, for the suggested voice solution, some people may not be able to speak due to injuries or mental deficiencies, and a person can lose his/her voice temporarily due to illness such as cold, cough, drunk, etc. Skin is also affected by several external factors such as temperature, illness, etc.

Voting system is an example which need to be resistant to coercion attacks. A voting system is coercion-resistant if it is not possible for the adversary to determine whether a coerced voter complies with her demands to vote in a particular manner. Different protocols have been proposed to achieve secure electronic voting systems. Blind signature [114], deniable encryption[115], and mix-net [116] are some of the proposed protocols. Blind signatures verify the validity of a document without revealing its content, using, e.g., RSA. Mix-net schemes permute and modify the sequence of objects in order to conceal any correspondence between them. Deniable encryption is a mechanism whereby the user can have multiple ciphertexts for an encrypted message which results in different plaintexts from the same ciphertext. These proposals aim to protect encrypted documents when the decryption key has been coerced from the user and it is known to the adversary. The Tacit Secrets approach protects the decryption key itself from coercion through communicating the key as the user does not have explicit knowledge of the key.

3.3 Methodologies in User Authentication

To validate my two proposals, a number of user studies are performed both in lab and online using Amazon's Mechanical Turk (MTurk) crowdsourcing service. I ran two different studies with 910 participants through in-lab and online sessions. In Section 3.3.1 I explain the details on using this platform for my proposes approach. To evaluate different usability, deployability, and security aspects of the proposed approaches, I used the UDS framework [3] which I also explain in Section 3.3.2.

3.3.1 Amazon Mechanical Turk Studies

Amazon Mechanical Turk [117] started in 2005 as a US-based microtask marketplace to "crowdsource" labour intensive tasks. MTurk is now being used as a source for hiring participants for research/experimental studies and provides a workforce on demand. This online labour market coordinates the supply for tasks that require human intelligence to complete. On this platform, those people who meet certain criteria for the designed tasks, aka HITs (Human Intelligence Tasks) are called "workers" and the ones who recruit the workers are called "requesters". Once the workers successfully complete HITs, if the requesters approve their submissions, they will receive monetary rewards (in U.S. Dollars). Both workers and requesters are anonymous although responses by a unique worker can be linked through an ID provided by Amazon.

Requesters can determine specific qualifications for HITs. A qualification is a property of a worker that represents a worker's skill, ability or reputation. These qualifications are used to control which workers can perform your HITs. HITs are visible only to qualified workers. For the proposed approach, I was looking for English speaking participants, so I limited the workers to be from English speaking countries.

When workers access the website, they find a list of tasks sorted according to different criteria, including the amount of the reward as well time allotted for the completion of each

HIT. Workers can read brief descriptions and see previews of the tasks before accepting to work on them. The speed of recruitment depends on the associated reward as well as the required amount of time.

Given the diverse demographic characteristics for MTurk workers, it potentially provides more realistic results compared to the lab studies which are often run in universities or colleges where the participants are less diverse (in terms of different attributes such as age, education, nationality, etc). In shorter period of time, a large number of participants are recruited in a less expensive manner. On the other hand, due to the importance of workers' reputation in this marketplace they always trying to have high approval rates for their submissions (i.e., approve or reject is done by the requester after workers complete a task) in order to be considered as master workers who they are paid more.

3.3.2 UDS Framework

To evaluate different aspects of the proposed approaches, I use Bonneau et al.'s usability-deployability-security ("UDS") framework [3]. This framework covers a broad range of usability, deployability, and security metrics. It allows researchers to conduct a broader evaluation of security solutions without biasing on just security or usability. For years, researchers have proposed several alternatives for authentication and claim their approach performs better than others. Using this framework, a more comprehensive evaluation of different benefits of the schemes will be performed when it comes to comparison of different alternatives. Based on this framework, if the scheme has the benefit a black circle is provided, empty circle means that the scheme almost offers the benefit. If there is no circle the scheme does not offer the benefit. I also added two other shapes to this framework using black and empty triangles. A black triangle means that the scheme has the potential for offering the benefit where as the empty triangle means the scheme has potential to almost offer the benefit. Here "potential" means that we have not enough data to support the claim; however, our theoretical analysis shows that the scheme can possibly offer the benefit. Bonneu at al. [3]

conducted their analysis for 35 password replacement schemes. Table 3.1 shows a shortened version of this framework for passwords, system-assigned passphrases, and biometrics.

Table 3.1 Shortened version of UDS framework for web passwords, system-assigned passphrases, and biometrics [3].

	Memorywise-Effortless	Scalable-for-Users	Nothing-to-Carry	Physically-Effortless	Easy-to-Learn	Efficient-to-Use	Infrequent-Errors	Easy-Recovery-from-Loss	Accessible	Negligible-Cost-per-User	Server-Compatible	Browser-Compatible	Mature	Non-Proprietary	Res.-to-Physical-Observation	Res.-to-Targeted-Impersonation	Res.-to-Throttled-Guessing	Res.-to-Unthrottled-Guessing	Res.-to-Internal-Observation	Res.-to-Leaks-from-Other-Verifiers	Res.-to-Phishing	Res.-to-Theft	No-Trusted-Third-Party	Requiring-Explicit-Consent	Unlinkable
Web Passwords			●		●	●	○	●	●	●	●	●	●	●		○						●	●	●	●
Sys-Asgn Passphrase	≡		●		≡	≡	≡	●	≡	●	●	●	≡	●		●‖	●‖	●‖		●‖		●	●	●	●‖
Biometrics-Fingerprint	●‖	●‖	●	○‖	●	○≡	≡	≡	○≡	≡	≡	≡	○≡	≡	●‖	≡	●‖			●‖	●‖	●	●	●	≡
Biometrics-Iris	●‖	●‖	●	○‖	●	○≡	≡	≡	○≡	≡	≡	≡	○≡	≡	●‖	≡	●‖			●‖	●‖	●	●	●	○≡
Biometrics-Voice	●‖	●‖	●	○‖	●	○≡	≡	≡	○≡	○≡	≡	○≡	○≡	≡	●‖	≡	○‖			●‖	●‖	●	●	●	≡

● – offers the benefit, ○ – almost offers the benefit, no icon – does not offer the benefit, ‖ – better than passwords, ≡ – worse than passwords

I used this framework to evaluate both proposed approaches in terms of usability, deployability, and security. I was also able to perform a thorough comparison of my approaches with other methods of interest.

Chapter 4

Tacit Secrets

Learning and memory are not necessarily dependent on intention and awareness. An abundance of human behaviour is, in fact, based on automatic learning [118] through inaccessible knowledge. This unconscious and implicit mechanism can result in learning of complex information in the absence of awareness. Providing a system-assigned authentication scheme that is enabled by implicit learning can provide several advantages. First and foremost increasing the level of security as user's choice is not involved. However, the problem with system-assigned secrets is memorability issues. To make a balance between security and usability, we involved an implicit learning-enabled authentication approach. The lack of awareness while learning occurs implicitly decreases the cognitive load on users. While we are living in an ever-increasing informational demands world, we need to manage the load on our mental system and improve performance of information processing. Implicit learning can help towards this goal to decrease the cognitive load. Moreover, implicitly acquired knowledge is resistant to several mental disorders which makes it beneficial to be used for authentication. Thus, evaluating how implicit learning can provide more distinctive patterns for the users in order to authenticate them has room for future studies.

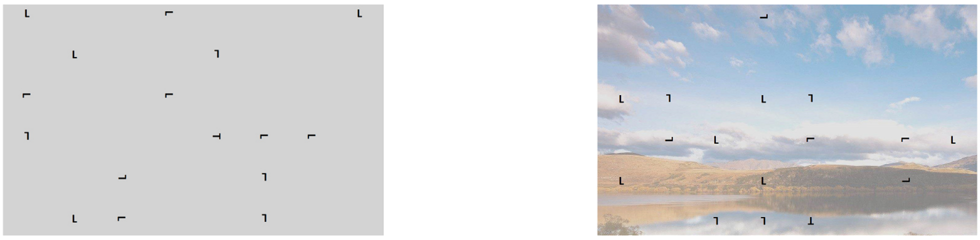
We have designed a completely new approach to system-assigned passwords, we call Tacit Secrets. This approach employs implicit memory and assigned passwords don't need to be explicitly remembered. These passwords are quite different than what we are used to the user plays a game to login. As discussed in Section 3.2.4, implicitly learnt knowledge is resistant to coercion attacks. Thus, implicitly learnt contexts of Tacit Secrets cannot be simply revealed even when the user is convinced or coerced. So, it can provide a coercion attack-resistant authentication scheme. In this section I explain more details about the design of the proposed approach and continue be providing the results.

4.1 Direct Implicit Learning-Based Authentication Secrets

Tacit Secrets, as a system-assigned authentication approach, uses the CC paradigm to implicitly learn the configurations of a random set of displays, which is later used for authentication purposes. The proposed approach employs implicit learning directly in order to assign users authentication tokens. The approach include two different phases, training and login. Users go through a training phase where their knowledge of the assigned key stabilizes. The learning process occurs implicitly in a way that users are not aware of how/what they have learnt. We evaluate the acquired knowledge in three different login sessions. The first session happens immediately after the training, the second and third sessions are scheduled for 24-48 hours and 7-8 days after the training session accordingly. To be consistent with previous authentication studies, we schedule the follow-up sessions to be 24-48 hours and 7-8 days after the initial training session.

4.2 User Task

Training (Registration). The goal of training is to ensure the user implicitly learns a set of displays; this is accomplished during account registration through a computer task. We use K_i to refer to user i's key, which is a set of randomly assigned displays. A display (aka. context) is considered as a 2-dimensional spatial configuration (i.e., placement) of irrelevant objects (aka. *distractors* - L letters) in which a target (T letter) is presented. We use N_i to



(a) Without background

(b) With background

Fig. 4.1 Illustration of different Tacit Secrets displays with and without background image.

refer to a sequence of novel displays; i.e., displays that are not in K_i for user i. We also use the notation R_i to refer to a sequence of displays shown to user i, where each display is drawn at random from K_i. In the training session, user i is shown R_i and N_i, which are interleaved at random. For each display, the user must search for a single rotated 'T' (the target) among many 'L's (the distractors; see Figure 4.1). Once the target is found, they must report the target orientation as quickly as possible by pressing the corresponding arrow key. Pressing the incorrect key, or not pressing any key, results in an invalid response for that display. There is a time limit of 3 seconds for each display that if the user does not answer, the display is removed and the new one is shown. At the end of the training session, the user is expected to have implicitly learnt the configuration for the displays in K_i.

Testing (Login). To be authenticated at a later time, a user i is provided with the same task as in training that contains a sequence of previously seen displays, R_i (which are randomly selected from K_i), interleaved with a sequence of random displays, N_i. By demonstrating better performance on the displays in R_i, the system validates a user's identity. For each display, a response is considered as incorrect if the target orientation is not correctly answered or if the time limit ends (i.e., 3 seconds). To evaluate each user's performance, we only consider performance data for the responses labeled as correct. Users only have one chance to find the target letter, 'T', and input its orientation for each display.

4.3 Design Considerations

Here we explain the design considerations and parameters for our Tacit Secrets experiment. We vary the parameters later to determine how optimized they can be later on in Sections 4.8.4 and 4.8.4.

Number of Displays per Session. The training phase consists of 240 trials (i.e., displays), divided into 15 blocks (i.e., repetition) of 16 trails. Of those 16, there are 12 repeated (user's key) and 4 novel displays on each block. There are 48 (i.e., invisible matrix of 6×8 - see Figure 4.2) possible target locations in each of the 16 trials in a block. As per the previous studies, for CC, for a display containing 1 target and 15 distractors, the matrix contains 6 rows and 8 columns [119–121]. We looked for an optimum number of repetitions to balance reliable implicit learning and the user's time. To find this number, we referred to previous studies on the CC paradigm and found that these studies (e.g., [121]) suggest that the cueing effect arises after the fourth block and there are no reliable trends in RT before this block. The decreasing trend for the RT would exist until block 15 and 16 [119, 120]. Although different studies have a different number of blocks, we were looking for the minimum and optimum number of blocks in which the best performance of users can be achieved. In a typical CC experiment there are usually 16 trials per block (i.e., 8 repeated and 8 novel). In order to increase each user's implicitly learnt key length, we increased the number of repeated displays such that each block contained 6 repeated, 6 repeated with background image, and 4 novel displays. These 12 repeated displays are considered as the user's key which are repeated through each repetition.

The first testing session happens immediately after the training phase. This session contains 40 displays: 20 repeated and 20 novel. Authentication succeeds if a user shows a statistically significant difference on the 20 repeated displays over the 20 novel displays. The follow-up sessions each contain 100 trials where half of them (i.e., 50) were previously seen and the other half were novel (see Table 4.2).

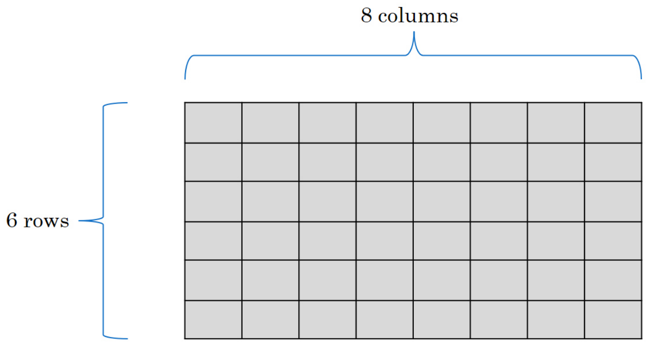


Fig. 4.2 Sample display for Tacit Secrets.

Table 4.1 The number of displays in different phases of the experiment per block.

	No. blocks	Repeated	Novel	Total
Training	15	12	4	240
Session 1	4	5	5	40
Session 2	10	5	5	100
Session 3	10	5	5	100

4.4 Verification of Tacit Secrets

To be authenticated at a later time, a user i is provided with the same task as in training. The sequence of novel displays in N_i are once again drawn randomly from $D \setminus K_i$, so they are unlikely to have been seen before. The sequence of displays in R_i are drawn again randomly from K_i (see Figure 4.3). By demonstrating better performance on the displays in R_i over the displays in N_i, the user i is demonstrating knowledge of the displays in R_i (and thus K_i). Figure B.6 shows how the relation between these sets and sequences are defined.

For each display, a response is considered incorrect if the target orientation is not correctly input within the time limit (i.e., 3 seconds). We only consider performance data for the responses labelled as correct. Users only have one chance to input a target orientation for each display.

Performance Data. We define performance as a measure of how quickly users respond to the stimuli. For performance data used in making authentication decisions, we use RT,

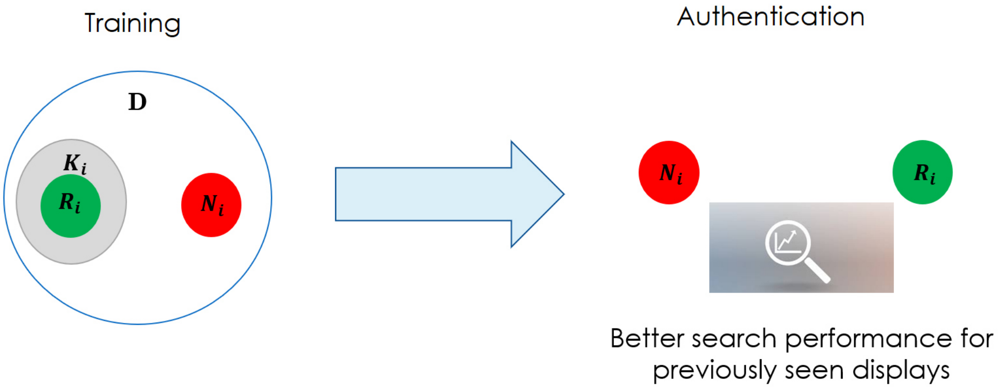


Fig. 4.3 Tacit Secrets Design. K_i, (user i's secret) displays drawn at random from D. N_i, sequence of novel displays drawn at random from . R_i: sequence of repeated displays drawn at random from K_i. Users have better search performance for R_i (previously seen displays).

and the eye tracking metrics of fixation counts and saccade counts. RT and eye tracking behaviors have been used in the cognitive psychology literature to measure CC IL effects, but averaged over the whole sample of participants rather than on a per-user basis. Outside of an authentication context, Chun et al. [45] found the general RT trend to be significantly lower over a set of subjects for repeated displays than novel displays. Zhao et al. [122] studied eye movement patterns when performing CC tasks outside of an authentication context. They performed their analysis over their whole sample of participants and note the group's trend is that repeated displays had improved performance, leading to significantly fewer fixations and saccades before the target was found.

We note that it may be possible in future work to incorporate further metrics, e.g., related to mouse movements or touch screen behaviours, depending on the environment.

Verification Method. We present verification methods that consider each metric alone, and all three in combination. For each metric alone, we consider login success to occur if the Mann-Whitney (MWU) test is significant with $\alpha = 0.05$. The null hypothesis for the MWU test is that the distribution of the performance metric (either RT, fixation count, or saccade count) for R_i is the same as for N_i, against the alternative hypothesis that the distribution of the performance metric for R_i is significantly different than for N_i. This test was chosen as it is nonparametric and the performance data (i.e., RT, fixation, and saccade count) is not normally distributed. Also, the performance data is ordinal. For all three metrics in combination, we consider login success to occur for user i, if i has significantly different patterns (using the MWU test, $\alpha = 0.05$) for at least two of the three authentication measures (i.e., RT, saccade, and fixation counts) on R_i vs. N_i. This approach has previously been used for challenge questions [123]. We note that we also evaluated the use of a KNN classifier, but its performance was inferior.

4.5 Eye-Tracking Data

An authentication scheme using eye movement has high resistance to observation attacks, and the information gleaned from an eye-tracker may also increase security. Eye tracking data can be properly acquired while a person is fully conscious (e.g., alcohol can affect eye movement). Therefore, duress or drugging a person to access a system might result in failure making its use appealing for coercion resistance.

For our proposed approach, we used Tobii Pro TX300 [124] device as a standalone eye tracker. The large head movement box allows the subject to move during tracking while maintaining accuracy and precision at a sampling rate of 300 Hz. This means that eye movements such as saccades and short fixations can be recorded. This device has a built-in user camera as well as a speaker which allows for recording of subjects' reactions to stimuli as well as playback of sounds. Accuracy under ideal conditions is measured in the center of the head movement box with the subject fixed in a chinrest. Data is collected immediately after calibration, in a controlled laboratory environment with constant illumination, with 9 stimuli points at gaze angles of $\leq 18°$.

Among different eye movements exhibited by the human visual system, the following three ocular parameters are most relevant to the purpose of our study: saccade (i.e., rapid eye rotation between fixation points) count, fixation (i.e., eye is stable toward the object of interest and the fovea remains centered on an object of interest) count, and average fixation duration.

4.6 Authentication Method

We hypothesized that due to the CC effect, user i would implicitly learn the configurations of their set of repeated displays (K_i), resulting in significantly better performance on the authentication measures for R_i (a sequence of displays drawn from K_i) compared to a sequence of novel displays (N_i). To test this hypothesis, we compared performance data from each user i for N_i versus R_i. If K_i has been implicitly learnt by the user, we expect better performance in finding the target for the displays in R_i than for the novel displays N_i.

4.6.1 Login Metrics

RT and eye tracking behaviors have been used in the cognitive psychology literature to measure CC IL effects, but averaged over the whole sample of participants rather than on a per-user basis. Outside of an authentication context, Chun et al. [45] found the general RT trend to be significantly lower over a set of subjects for repeated displays than novel. Zhao et al. [122] studied the eye movement patterns that exist in performing CC tasks outside of an authentication context. They performed their analysis over their whole sample of participants and note the group's trend is that repeated displays had improved performance, leading to significantly fewer fixations and saccades before the target was found. It is our goal to determine which of these metrics (alone or in combination) produces the most accurate measures of IL using CC, in order to design an IL-based authentication system with promising accuracy, training times, and login times. As such, we study each login metric alone and in combination, on a per-user basis, in Section 4.8.

4.6.2 Statistical Test

The statistical test used by the Tacit Secrets system's performance metric comparisons was chosen based on some assumptions. Firstly, the performance data is not normally distributed so a nonparametric test is sensible. Secondly, the measurement scale of the dependent variable (i.e., each type of performance data, for each user, for each display) is ordinal. The Mann-Whitney U (MWU) test is used to understand whether the performance metrics, i.e., RT, fixation, and saccade count, differ based on display type for a given user i. Here the dependent variables are RT, fixation count, and saccade count; and the independent variable is display type, which can be either repeated (i.e., in R_i) or novel (i.e., in N_i). The null hypothesis for the MWU test is that the mean of the performance metric (either RT, fixation count, or saccade count) for R_i is the same as for N_i, against the alternative hypothesis that the mean of the performance metric for R_i is significantly different than for N_i. We ran the test on the recorded data of each user i for every session.

4.7 Experiment

Here we describe our experiment to test the Tacit Secrets design. The experiment ran over two weeks in a laboratory environment in order to collect eye-tracking data.

4.7.1 Participants

Thirty participants (18 males and 12 females, aged between 18 and 25 years) were recruited through email and posters which were distributed across the university campus. These participants were paid \$10 each to participate in our lab study and entered into a draw for \$50. The inclusion/exclusion criteria consisted of being with normal or corrected-to-normal vision acuity, and not to be registered in any computer security-related program. All of the participants were students, where 67% of the participants had a high school degree (or equivalent) and 33% had a university or college degree. 30% of the participants majored in engineering and applied science, 30% science, 23% business and IT, and the other 17% majored in health and social science. 53% of our participants had normal and 47% had corrected-to-normal vision.

4.7.2 Study Structure and Organization

The participants were asked to attend three sessions. The sessions were scheduled according to the participant's convenience, within the following constraints: the second session is two days after the first training session, and the third session happens a week after the second session. The procedures for all three experimental sessions were the same except that the pre-experimental questionnaire is only presented during the first session.

Participants were instructed to sit approx. 60 cm from a 23-inch LCD display monitor with a sample rate of 85 Hz and to press a keyboard in response to stimuli. In the first session, participants were asked to sign the consent form and then were provided written and oral instructions. They were calibrated with the eye-tracker and started using the application after they agreed to their participation in the experiment. The study purpose (in the consent form and invitation letter) was left intentionally vague, so they were not informed about the exact process of learning that the experiment was testing until after the end of the experiment. The reason for this was that we wished to avoid the possibility of this knowledge affecting their performance and thus the unconscious learning that the experiment aims to test. The experiment's purpose was debriefed at the end of the third session. The experimental procedure was approved by the Research Ethics Board at our university.

During the pilot testing, we realized that in addition to a mandatory break that is given between the training and testing phase, the task needs to provide users opportunities to have optional rest-break when they felt tired. This rest-break is taken by pressing the 'Esc' key during the entire experiment. By pressing 'Enter' they can continue afterwards.

Training Phase (Registration). During the training phase, when users start the CC task, a block of 12 displays are assigned to them to be repeated and used for the authentication process. These 12 displays are the implicitly learnt "key" for the rest of the experiment. In each block (of 16 displays), the 12 repeated displays are shown in scrambled order and the other 4 displays are novel and changed in each block. All displays including repeated and novel are scrambled through each of the 15 blocks. Upon completion of the training phase, users were provided a 5 minute break along with a demographic questionnaire to fill out. This questionnaire was only given in the first session of the study. After filling out the questionnaire, they started the testing phase.

Testing Phase (Login). The first testing session happens shortly after the first training session, in the same sitting. The trainees' knowledge was also assessed to see whether the learnt information persists over time (two days and one week after the first session).

4.7.3 Design Considerations

Here we explain the design considerations and parameters for our Tacit Secrets experiment. We vary the parameters later to determine how optimized they can be later on in sections 4.8.4 and 4.8.4.

Number of Displays per Session. The training phase consists of 240 trials (i.e., displays), divided into 15 blocks of 16 trials, of those 16 displays, there are 12 from R_i, and 4 from N_i in each block. Figure 4.4 indicates an example of how displays are exposed in each block during the training session. In each display, there are 48 (i.e., invisible matrix of 6×8) possible target locations.

We looked for an optimum number of repetitions of each display type to balance reliable implicit learning and the user's time. To find this number, we referred to previous studies on the CC paradigm and found that these studies (e.g., [121]) suggest that the cueing effect arises after the fourth block of 16 displays, and there are no reliable trends in RT before this block. The decreasing trend for the RT would exist until block 15 and 16 [119, 120]. Although different studies have a different number of blocks, we were looking for the minimum and optimum number of blocks in which the best performance of users can be achieved.

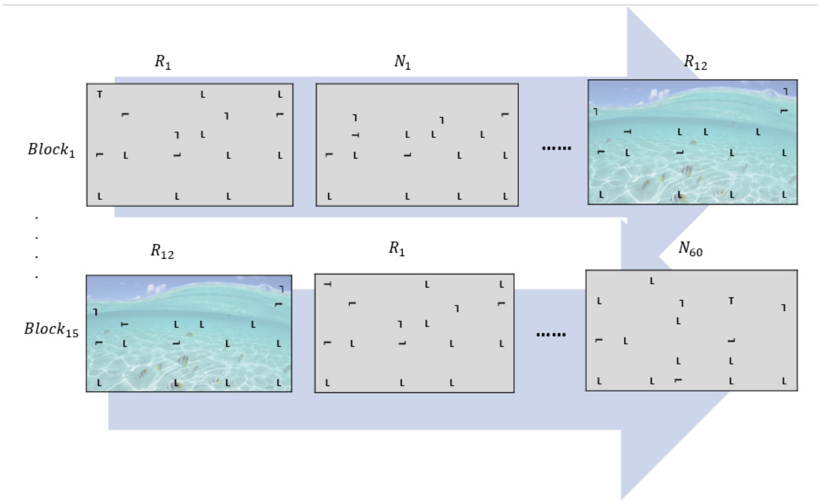


Fig. 4.4 An example of displays arrangement during the training sessions.

Table 4.2 The number of displays in different phases of the experiment per block.

	No. blocks	Repeated	Novel	Total
Training	15	12	4	240
Session 1	4	5	5	40
Session 2	10	5	5	100
Session 3	10	5	5	100

The first testing session happens immediately after the training phase. For each user i, this first session contains 40 displays: R_i contains 20 displays and N_i contains 20 displays. Authentication succeeds if a user shows a statistically significant difference in performance on R_i versus N_i. The follow-up sessions each contain 100 trials where R_i contains 50 displays drawn randomly from K_i, and N_i contains 50 random displays (see Table 4.2).

The more an attacker attempts to pass authentication, the more probable it is that he could learn more displays. Doubling the number of learnt displays in K_i from 12 to 24 would result in a key space of 2^{1001}. Since each display is a 6×8 matrix, there are 48 possible positions on each display where objects (distractors or targets) can be placed. Each display contains 16 objects; 15 distractors ('L') and 1 target ('T'). First, the position of the target is chosen: ${}_{48}C_1$. Then the position of each of the 15 distractors is chosen: ${}_{47}C_{15}$. Thus,

$|D| = 48 \times {}_{47}C_{15} = 2^{45}$. Given that there are 24 displays to be chosen from D, the total number of possible keys is: ${}_{2^{45}}C_{24} \approx 2^{510}$. Thus, a brute-force offline attack is expected to succeed only after approximately 2^{1000} guesses. This key space means that the attacker would need to memorize more displays if he knows (e.g., by observation) the authentication displays of a legitimate user during an authentication session. However, such an increase would require a longer training period. Another variation to harden the system is to change the number of novel and repeated displays shown in the sequences N_i and R_i respectively for login; for example, instead of having an equal number of repeated and novel displays (i.e., 50), we could halve the number of repeated displays (i.e., to 25) and increase the number of novel displays (say to 75). This variation would result in an attacker requiring to have an improved performance in 25 out of 100 displays. Furthermore, this variation would reduce the number of learnt displays that get exposed in one single authentication session (see Section 4.9 for further discussion). The number of the stimuli that are presented to the user through the course of the authentication phase, which can be tuned to different levels of security (see Section 4.9 for a discussion of some ways these parameters could be tuned).

Display Variations. The Tacit Secrets task contains four different variations of displays of size 1440×900 pixels, including array and scene-based novel displays that do not involve any CC effect, array-based (standard CC) repeated displays, and scene-based repeated displays which contained a background image (see Figure 4.1b). Scene-based displays elicit scene-based cueing, which is related to a background scene and array-based cueing occurs based only on the position of distractors in the context. Brooks et al. [125] suggest that when a particular repeated array had been consistently associated with a particular scene background, it produces more robust contextual cueing. They found that training with scene-array displays led to joint learning of the two cues, such that cueing was disrupted when either the scene or the array is changed. In our experiment, we used natural scenes as backgrounds for half of the repeated displays. The reason to have half of the displays with and other half without a background image, was to see how the participants performance for different types of the displays would be affected based on different display types. Once a background image is assigned to a repeated display, the display would be always presented with that same background image. These images were randomly chosen from our database. Participants searched for a target that was predicted by both the background scene and the locations of distractor items. We also adjusted the luminance of the target and distractors across displays in order to increase search items' contrast against the background scene. In all displays, the target appears equally likely in each of four quadrants of the screen to eliminate learning of location frequencies for the repeated stimuli.

Search Strategy. To facilitate access to implicit knowledge, thereby allowing a consistent Contextual Cueing Effect to develop, we asked our subjects to use a passive strategy while searching for the target. Smilek et al. [126] studied how cognitive performance can be improved when subjects are instructed to be passive and not to 'try hard'. Thus, we notified them that the best strategy for this task is to be as receptive as possible and asked them to "let the unique item pop into your mind as you look at the screen". Lleras et al. [38] hypothesized that using different search strategies: active (an active effort to find the target) vs. passive (intuitive search, wherein they need to be as receptive as possible, let the unique item 'pop' into their mind while looking at the screen, let the display and intuition determine the response, and tune into 'gut feeling'), can have different results while performing the CC task. They experimentally showed that those subjects who used a passive strategy for the search task had more substantial CC effects. We do not know what strategy users really used; however, providing a set of precise and consistent instructions helps us guide users from arbitrarily choosing a search strategy.

Positive/Negative Feedback. To indicate that a user's response has been recorded by the system, after pressing a key, a border appears around the display which is either green (when the correct arrow is pressed) or red (when an incorrect arrow is pressed). This decision follows Lleras et al. [127], who investigate how contextual learning is considerably sensitive to external rewards associated with the search interactions. Rewards can be provided in form of a tone or visual feedback that indicate correctness of user's responses (positive or negative).

4.8 Analysis and Results

Here we seek answers to the following questions: how well does Tacit Secrets perform for implicit-learning based authentication in terms of (1) authentication success rates, (2) false positives, and (3) speed for different system configuration?

We first analyze the general trends in performance data for the entire sample of participants. Then we examine using RT as a single measure for authentication. Next, we analyze the success rates by using eye tracking measures (fixation and saccade count) as additional measures for authentication. We later expanded our authentication measures to three by incorporating two eye tracking measures (fixation and saccade count). We then analyzed Tacit Secrets for an optimal configuration given (1) RT as a single measure and (2) RT along with eye tracking measures.

4.8.1 General Performance Data Trends

RT Performance. To confirm the CC effect, we first analyze the search RT for the entire sample of participants. Figure 4.5 indicates descriptive statistics which summarize the participants' RT for different sessions including the training and login sessions. Figure 2.2 indicates the overall RT performance for the repeated displays compared to novel ones for all our participants.

False Positives

Since the scheme uses reaction time as a measure to identify a user, its accuracy should also be evaluated in terms of the false acceptance rate (FAR), i.e., the proportion of attempts

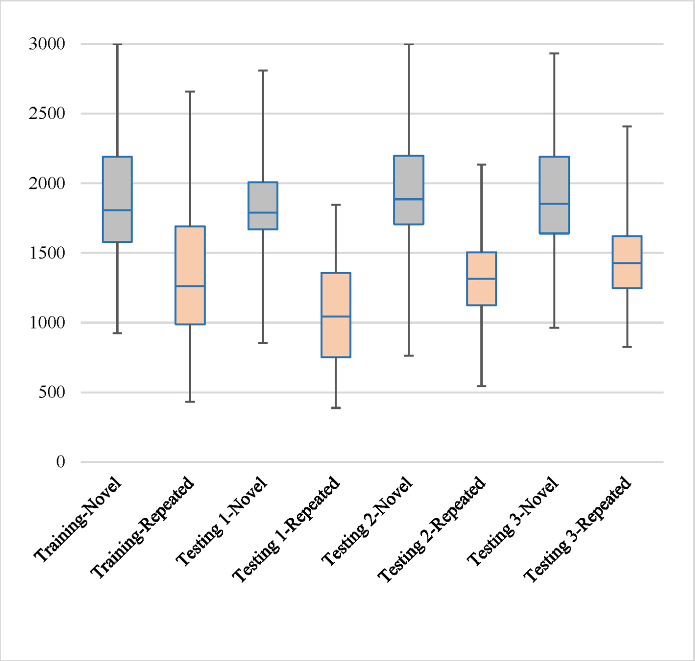


Fig. 4.5 Box-and-whiskers plot showing RT (in milliseconds) summarizing all data collected for 30 participants for each session.

wrongly classified as legitimate. As some of our participants did not attend some of their testing sessions, our analysis in this section is based on the sessions they attended.

To evaluate this threat model, we used each user's display sequence labels (i.e., 'novel' and 'repeated') to re-label each other user's sequence and see if the newly-re-labelled sequences passed or failed authentication. In our designed approach, different users have different sequences, containing a different order of display types. In this scenario, we assume attackers try to use their own performance data to login to another user's account. Our three authentication sessions had a different number of displays: 40, 100, and 100 for Session 1, 2, and 3 respectively. Thus, we did the analysis through labeling each subject's display sequence for Session 1 with the Session 1 display sequence of all other users, and the display sequence of Session 2 and 3 of each user with the display sequence of Session 2 and 3 of all other users. As shown in Table 4.3, through the first run of the test, we considered all types of displays, including array-based repeated, scene-based repeated, and novel displays. Then, we excluded scene-based displays to see if the results changed. The exclusion was due to the possible complexity that displays with background image might have which could cause poor performance of the users. As the results show, there is a negligible improvement of 0.2% in the false acceptance rate when we excluded background displays.

Table 4.3 The number of cases the MWU-test passed -False Positives (S_1: Session 1, S_2: Session 2, S_3: Session 3).

Display Types	S_1-S_1	S_2-S_2,S_3	S_3-S_2,S_3	Total	Passed
All Types	70/870	137/1404	147/1566	3840	9.21%
Exclude BG	60/870	127/1404	160/1566	3840	9.03%

We further improve the false positive rates through using eye-tracking data and evaluate different configurations of Tacit Secrets in Section 4.8.4.

Speed

This refers to how quickly users can accomplish the task. The mean training time was 14.5 minutes which appears to be about $\frac{1}{3} - \frac{1}{5}$ of the mean training time for the SISL task (30-45 minutes) [31]. We further improve the login time through different configurations of Tacit Secrets in sections 4.8.4 and 4.8.4.

Table 4.4 The median, mean and standard deviation time for each session.

	Training	Session 1	Session 2	Session 3
Mean	14:49	01:08	04:46	05:53
Median	14:18	02:09	04:14	05:40
Std. Dev.	02:46	00:29	01:36	00:24

4.8.2 Results Using Eye Tracking Metrics

Authentication Success Rate

Here we analyze the eye tracking metrics to see how many users would authenticate successfully if these metrics were used alone. Table 4.5 indicates the percentage of the subjects who showed significantly different patterns for each of these eye movements for R_i versus N_i in each testing session. We use the MWU test (at $\alpha = 0.05$) for each of these sessions. So, our results confirm that the fixation and saccade counts were fewer for the repeated displays R_i than the novel ones N_i for our entire study population (on average). We did not find a shorter fixation duration for the repeated displays.

Table 4.5 The percentage of the subjects whose eye movement measures for novel and repeated displays are significantly different for each session.

	Session 1	Session 2	Session 3
Fixation count	79.31%	86.21%	72.41%
Saccade count	89.66%	75.86%	76.29%

As Table 4.5 indicates, these eye movement measures show promise for improving the performance of Tacit Secrets; however, its authentication success rates alone are not better than using RT. Thus, we investigate methods of combining this information with RT in Section 4.8.3.

Note that the false positives were not studied here as the authentication success was lower than for RT alone, so instead we study it in combination with RT in Section 4.8.3.

4.8.3 Results Combining RT and Eye Tracking Performance Metrics

In this section, we discuss how Tacit Secrets performs by using all three performance metrics (RT, saccade count, and fixation count). We evaluate two different approaches for incorporating eye movement measures. Our direct implicit learning-based authentication tokens approach using a classification algorithm is discussed in Section 4.8.3. In Section 4.8.3, we explain another approach that simply evaluates whether the user has significantly different patterns for at least two of the three authentication measures (i.e., RT, saccade, and fixation counts) on repeated vs. novel displays. This approach has previously been used for challenge questions [123]. This approach had the best performance.

Also note that in Section 4.8.4, we determine how different configurations of displays would result in different success rates when considering the three performance metrics.

KNN Classifier

To find out how the three features can be used to distinguish display types, we first used the K-Nearest-Neighbours (KNN) classifier. This classifier labels the displays (i.e., novel and repeated) based on their user's RT, fixation, and saccade counts. We applied the classifier on each user's testing sessions. For the KNN classifier we tested values of *k* between 1 and 20 and weighting samples by Euclidean distance. The best results were achieved with *k* between 2 and 11 for all datasets. We gained an average of 85% accuracy for this classifier to label all the data. Given the recorded indicators for each session, the classifier labels the data, and the user can be identified based on demonstrated knowledge of the user's key (i.e., learnt displays). However, since the accuracy is not perfect, there needs to be a threshold of how close the classified input key must be to the actual user's key.

We use the Hamming distance thresholds between each user's actual key and the identified key predicted by the KNN classifier. The Hamming distance is interpreted as the number of bits which need to be changed (corrupted) to turn one string into the other. This number varied between 8 to 30 for our participants' recordings.

To find the best threshold in which the system using this approach has the best performance in terms of FPR and TPR, we plotted a ROC curve for each testing session separately. Given various thresholds for each session, we compared each user's actual key with all other users' predicted keys to find the Hamming distance between those keys. Given the particular threshold, we found whether the system passes or fails the user's identity by comparing the keys. Our analysis showed the best performance was achieved at threshold 22 and 20 for testing Session 2 and Session 3, respectively. Figure 4.6 and 4.7 indicate the ROC curves for different thresholds we tested for Session 2 and 3, respectively.

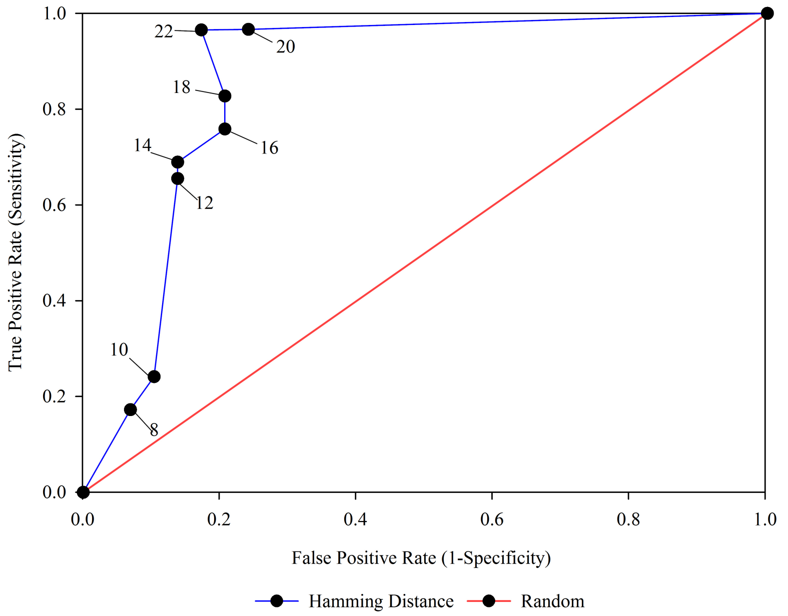


Fig. 4.6 ROC curve for Tacit Secrets performance using the KNN classifier given different thresholds for Session 2.

In general, the findings show that while this method can increase TPR slightly, it also has a negative effect of increasing FPR. Thus, we investigate another approach of incorporating eye-tracking measures in Section 4.8.3.

Authentication Measures Subset

Here, we consider verifying each user's identity if a significant difference in two of the three authentication measures (i.e., RT, fixation count, and saccade count) confirm the user's legitimacy. Given such an assumption, a user passes Tacit Secrets if there is a statistically significant difference between their performance data for the displays in R_i versus N_i on at

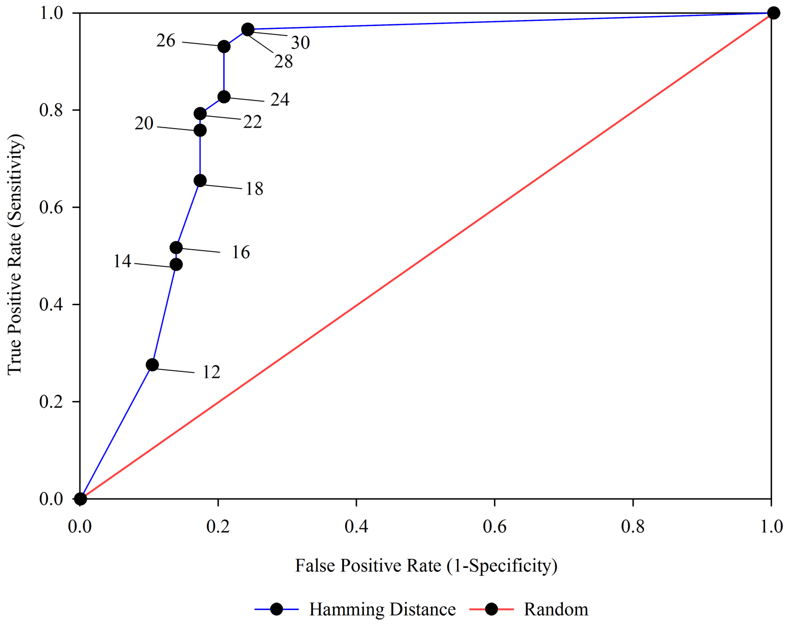


Fig. 4.7 ROC curve for Tacit Secrets performance using the KNN classifier given different thresholds for Session 3.

least 2/3 of the indicators. Using this rule, the authentication success rate was improved for both Sessions 2 and 3 with 96.15% and 92.86% success rate for these sessions respectively. The success rate improvements are comparably better than considering RT solely (which were 88% and 86% for sessions 2 and 3 respectively). We further consider changing the number of displays in Section 4.8.4 to determine an optimal overall Tacit Secrets configuration and evaluate false positives and speed there as well.

4.8.4 Testing Optimal System Configurations

Tacit Secrets Configuration: Authentication based on RT

Since the testing time with the basic configuration of the system (i.e., 50 displays in R_i and 50 displays in N_i displays) was quite long in comparison with traditional authentication schemes, we simulated different combinations of display numbers to determine if the system can perform better while the number of displays for the testing session was changed. The way we sampled data for this purpose was to randomly select from each user's Session 2 and 3 datasets. Such sampling can provide us a good estimate since we are not sampling based on the high performance results from the immediate testing session (i.e., session 1); on the other hand, since the sample is taken from testing sessions 2 and 3, the measurements may be influenced by both higher learning effects from more repetitions and also higher fading effects due to the time delays. Such sampling makes more variability on the data, which may, if anything, reduce the success rate of our tests. In addition, there is not a remarkable RT improvement of the users from Session 2 to 3. Under this sampling method, the sequences of novel and repeated displays for every user differs in these simulations from the ones actually provided during the testing sessions.

We found by changing the different parameters (number of novel vs. repeated displays) can result in the same success rate value of the basic system parameters while having fewer displays, leading to a shorter testing session. One of the elements we considered in forming different configurations was including fewer repeated displays (users' learnt displays) which reduces the risk of observation attack. Hence, we selected 36 different combinations of display types with four different fractions of the displays, including $1R$(Repeated) $-1N$(Novel), $1R-4N$, $1R-5N$, $1R-7.3N$.

Furthermore, to evaluate the performance of Tacit Secrets, we used a Receiving Operating Characteristics (ROC) graph to compare Tacit Secret authentication performance against a random guess attack. This graph demonstrates the trade-off between True Positive Rate (TRP or Sensitivity) and False Positive Rate (FPR or 1-Specificity). For Figure 4.8, we selected 12 (out of 36) configurations that had an authentication success rate over 70% and calculated TPR and FPR for them. Figure 4.8 depicts the resulting ROC graph. It shows how different configurations of Tacit Secrets would perform in terms of TPR and FPR. The closer the points are to the northwest of the graph the better performance the configuration has. Based on the graph, the configuration with 25 repeated and 25 novel displays outperforms the other configurations with 0.897% TPR and 0.008% FPR. Given the 25-25 configuration, we can reach a strong performance, yet shorter session duration which improves the system's usability.

As shown on the ROC graph, the best performance is achieved for the 25-25 configuration; we next compare the performance of this configuration with the basic 50-50 configuration. The average login time for the 25-25 configuration would be 2.5 minutes which is comparably shorter than the 50-50 configuration average login time (5 minutes).

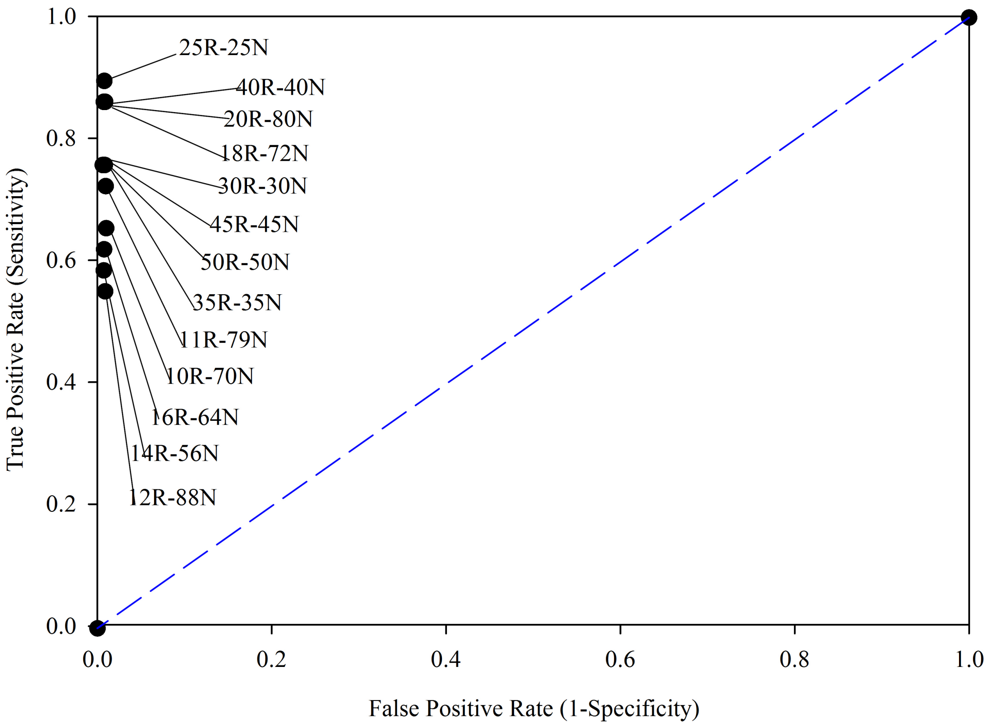


Fig. 4.8 ROC graph showing performance given different login configurations when using RT alone. Configurations are described by the number of novel (N) and repeated (R) displays they contain.

Tacit Secrets Configuration: Authentication based on RT and Eye-tracking Data

In this section, we investigate whether we can further reduce and optimize login time by using the approach of Section 4.8.3 to incorporate eye-tracking measures and altering the number of displays as in Section 4.8.4.

Using the same sampling mechanism as Section 4.8.4, 16 different configurations were analyzed for FPR and TPR to plot the ROC graph and find the best configuration in which the system has the highest performance. Figure 4.9 illustrates the performance of Tacit Secrets as the configuration of the system is varied. As the plot shows, there are 6 configurations, $25R-25N$, $40R-40N$, $10R-20N$, $20R-40N$, $20R-20N$, and $30R-30N$ which outperform the other. Since they have almost identical performance (0.966% TPR and 0.004% FPR), we select the one which has the lowest number of displays and also fewer repeated displays than novel to lower the observation attack risk. Thus, we recommend the configuration $10R-20N$ which contains 10 repeated R_i and 20 novel N_i displays. This configuration also results in a reduced login time which would be at most 2 minutes and on average 1.5 minutes.

The results in Figure 4.9 show a notable improvement compared with the results in which only RT was taken into account. In Section 4.8.4 we found the configuration with 25R-25N had the best performance; however, our analysis in this section revealed configurations with higher performance, with even fewer displays. The average login time for this configuration would be 1.5 minutes which is comparably shorter than the 50-50 configuration average login time (5 minutes). These results suggest amendments to Tacit Secrets's basic configuration to improve usability.

4.9 Security Analysis

In this section, we first provide our threat model in Section 4.9.1 and then analyze how our approach to Tacit Secrets would fare against five different attack scenarios. These attacks include: (1) offline brute-force in Section 4.9.2, (2) online guessing using population statistics

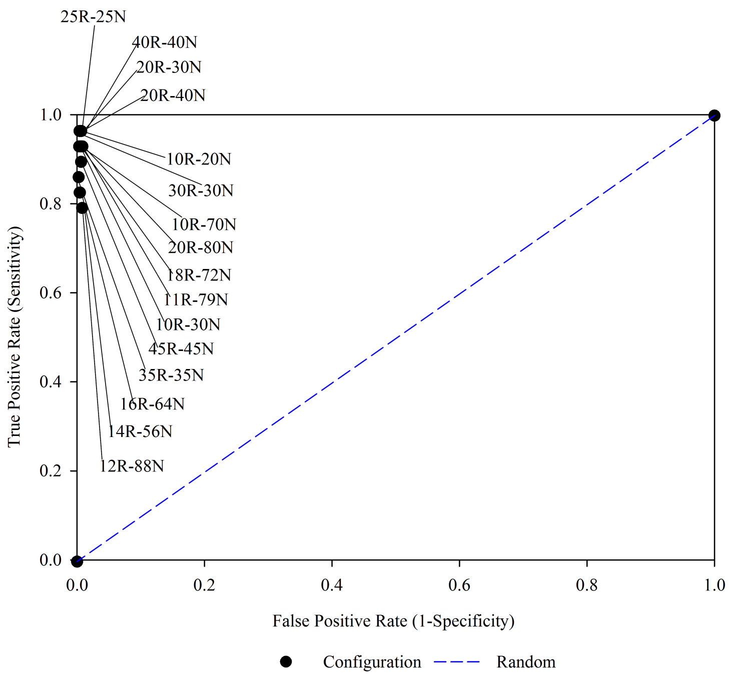


Fig. 4.9 ROC graph for Tacit Secrets performance given different configurations, incorporating eye-tracking measures as discussed in Section 4.8.4.

in Section 4.9.3, (3) coercion attacks in Section 4.9.4, (4) observation (shoulder-surfing) attacks in Section 4.9.5, and (5) phishing attacks in Section 4.9.8. Our security analyses are performed for both (1) RT performance data, and (2) RT and eye-tracking performance data.

4.9.1 Threat Model

Tacit Secrets provides a mechanism wherein a secret key is implicitly learnt by the user. Our threat model is based on the assumption that an adversary wishes to obtain the user's key in order to either decrypt previously collected data and/or gain access to a high security system, room, or administration task. Here we list the key assumptions which our analysis builds upon:

1. The attacker aims to compromise a user's account through an online attack.

2. The attacker uses software which is capable of (*i*) detecting background scene change, (*ii*) detecting display/context objects' orientations (using OCR), and (*iii*) responding with a chosen true delay.

3. The attacker is able to collect data from the population on the task in general (i.e., for both novel and repeated displays) to obtain response time distributions.

4. The attacker does not know what the display types are (novel/ repeated) for the target user.

4.9.2 Brute-Force Attack

Here we compare the security of Tacit Secrets with a previously offered implicit learning-based authentication scheme (i.e., the SISL task [31]). We compare the number of possible keys that can be assigned to users on each system. Bojinov et al. perform their analysis based on a counting argument of the number of possible sequences of 30-characters using the BEST theorem for the Euler cycle. They explain that the learnt sequence has about 38 bits of entropy which is far more than the entropy of the traditional user-chosen password. The learnt 30-character sequence in the SISL task is analogous to the 12-display set learnt in Tacit Secrets. Thus, for comparison, we first calculate the number of all possible displays that can be generated for use in Tacit Secrets.

In Tacit Secrets authentication, we need to store each display's arrangement of objects in the server. For each of the 12 displays of a user's key, we store a set of object (distractors and target) information. We call each set D_i, for $i = \{1 \dots 12\}$. D_i contains 16, 3-tuple elements, each representing an item on the display:

$$D = \{\{t, l, o\}, \dots\}$$

where t denotes item type (i.e., distractor or target), l denotes location (since the items are placed in a 6×8 matrix there are 48 possible locations), and o denotes the orientation of the item (i.e., left, right, up, and down). Each set is serialized and converted to a string. The string is then encrypted and stored on the server using a Tamper-Resistant Security Module (TRSM) on the server to store the user's private encryption key.

To determine the efficacy of an offline brute-force attack, we assume the attacker has the encrypted file and tries to guess the key so we must enumerate the size of the key space for our approach. We can consider a random, system-assigned Tacit Secret as set of size 12 (i.e., $|K_i| = 12$). Each element in K_i could be any display in D, with equal probability as it is system-assigned. To enumerate the key space, we must first determine $|D|$. Since each display is a 6×8 matrix, there are 48 possible positions on each display where objects (distractors or targets) can be placed. Each display contains 16 objects; 15 distractors ('L') and 1 target ('T'). First, the position of the target is chosen: ${}_{48}C_1$. Then the position of each of the 15 distractors is chosen: ${}_{47}C_{15}$. Thus, $|D| = 48 \times {}_{47}C_{15} = 2^{45}$. Given that there are 12 displays to be chosen from D, the total number of possible keys is: ${}_{2^{45}}C_{12} \approx 2^{510}$. Thus, a brute-force attack is expected to succeed only after approximately 2^{509} guesses.

Bojinov et al. evaluate their model for the basic coercion attack and explain how the required time for intercepting a group of trained users and making them reveal their key and using the revealed secret for authentication, takes one year of non-stop testing per user that has a little chance of success. They presume an attack scenario that occurs after the user has gone through the training process. Given that Σ is the number of possible secret keys, if the attacker intercepts u trained users and asks each q queries, he has a success probability of $qu/|\Sigma|$. Since a SISL login session takes about 5 minutes, they assume an upper bound of 10^5 queries per user. Thus, the probability of successfully finding one secret key from 100 users would be: $100 \times 10^5/|\Sigma| = 2^{-16}$. Since the authentication procedure for the SISL task is analogous with Tacit Secrets; that is, they are both based on the implicitly learnt key that is resistant to coercion attack, we can follow the same threat model and compare SISL with Tacit Secrets. We assume an attacker tries to intercept 100 users and ask them 10^5 queries, then the success probability would be:

$$100 \times 10^5 / 2^{45} = 2^{-26}$$

which is lower than the success probability of SISL task (i.e., 2^{-16}). Thus, these analysis confirms the high theoretical key size which is considerably larger than the key size provided by another proposed implicit-learning based scheme [31].

4.9.3 Online Attack Using Population Statistics

For an online attack to succeed, the attacker must correctly guess the type of all displays presented in a login session (i.e., if they are novel or repeated). If, as assumed in Section 4.9.1, the attacker knows the time distribution of novel/repeated displays, he/she can submit a legitimate guess for each display, and the attack success is determined by correctly guessing the type of each display.

To calculate the probability of correctly guessing all the display types in a session for user i, consider that there are $|R_i|$ positions from the sequence of $|R_i| + |N_i|$ displays that could contain the repeated displays. Then there are $_{(|R_i|+|N_i|)}C_{|R_i|}$ possible positions for the repeated displays. If the attacker has one attempt at guessing this particular sequence, since it changes on each login attempt, the probability of a successful guess of the entire display sequence is $1/(_{(|R_i|+|N_i|)}C_{|R_i|})$.

Using RT. ***(50-50 Configuration)***. Here $|R_i| = 50$, $|N_i| = 50$, and $|R_i| + |N_i| = 100$. Thus, the probability of a successful online guess is 2^{-96}.

Using RT. ***(25-25 Configuration)***.

We evaluate this configuration as we found it to outperform other configurations that only consider RT performance data (recall Section 4.8.4). Here $|R_i| = 25$, $|N_i| = 25$, and $|R_i| + |N_i| = 50$. Thus, the probability of a successful online guess is 2^{-47}. While this indicates this configuration is not as resistant to attacks as the 50-50 configuration, it is still sufficient to be considered resistant to online attacks [128].

Using RT and Eye-tracking Data. ***(10-20 Configuration)***.

We evaluate this configuration as we found it to outperform all other configurations (recall Section 4.8.4). Here $|R_i| = 10$, $|N_i| = 20$, and $|R_i| + |N_i| = 30$. Thus, the probability of a successful online guess is 2^{-25}. While this indicates this configuration is not as resistant to attacks as the 50-50 or 25-25 configurations, it is still sufficient to be considered resistant to online attacks [128].

An authentication token can withstand online attack if it cannot be revealed within 2^{20} guesses [129]; thus, for the attacker to succeed there is a probability of $1/2^{-47}$ which confirms our approach is resistant to online attacks.

4.9.4 Coercion Attack

Imagine a scenario whereby a motivated attacker threatens a legitimate user with a weapon or using blackmail. The attacker can ask the victim to hand over his/her key, or tailgate the user, e.g., through a physical access control point or forcing the user to login while he/she is present in order to take over the account after authentication is complete. Below we further explain these attack scenarios.

Communicating the Secret

This describes when a victim is forced to hand over his/her secret key so the attacker can masquerade as the user at a later time. Since our approach to Tacit Secrets is based on implicit knowledge, even if the trainee is coerced and willing to reveal the key, she/he is not able to do so as she does not have explicit and conscious knowledge of the key. The implicit nature of the acquired knowledge allows protection against such coercion attacks.

Tailgating

This describes when an attacker tailgates the user to the authentication station, coerces the user to login to the system, and then follows them past the authentication point. In this scenario, we have no evidence that our approach will protect the user's account, as the user may have no choice but to login out of fear for their life. To protect against such an attack scenario, we suggest using a type of panic password [111]. We note that it is also conceivable that our approach might provide some protection against coercion even in this scenario. Although it is not yet tested, it is possible that a user might fail to do the task properly as their subconscious system might be affected under duress (e.g., being stressed) [100]. Gauging the stress level of users and how duress influences the measurements of our approach is out of the scope of our feasibility study and is left as future work.

4.9.5 Observation Attack

Another type of attack can occur through an attacker's observations. Assuming that the training session is performed in a secure location, the attacker attempts to pass the login test using obtained knowledge through observations of single or multiple testing sessions. Given that he does not have any prior knowledge, he tries to recover the user's dataset through observation. So to have a probabilistic view of this threat, we consider the two following scenarios:

4.9.6 Single Observation

Through the first scenario, we assume the attacker observes one single login session and we want to know how much knowledge he might acquire through that session. Each user has a learnt dataset containing 12 displays' configurations. Through an authentication session, repeated displays will be randomly drawn from the set of 12, 50 times. If a display is shown at least twice, an observer can understand that it is a part of the user's learnt dataset. So we need to find the probability of exposing each display more than once. As there are 50 displays randomly selected from the user's set then P(occurring at least twice) = $P(X \geq 2) = 1 - P(X \leq 1) = 1 - binompdf(n, p, r)$ where *binompdf* is the binomial probability density function, n is the number of cued trials (i.e., repeated displays through a testing session), p is the probability of correctly guessing the display is a learnt display out of 12 learnt displays, and r is the number of successes (i.e., number of times a learnt display is exposed).

$$1 - binompdf(50, 1/12, 1) = 0.92$$

Additionally, for the novel displays the probability of each display to be displayed more than once is:

$$P(X \geq 2) = 1 - P(X \leq 1) = 1 - binompdf(n, p, r)$$

$$= 1 - binompdf(50, 1/2^{49}, 1) \simeq 0.$$

Through the aforementioned analysis, we find the probability of the attacker to recognize a display as the user's learnt display during a single observation.

4.9.7 Multiple Observations

Authentication based on RT. ***(50-50 Configuration)***. Another type of attack can occur through an attacker's observations. Assuming that the training session is performed in a secure location, the attacker attempts to pass the login test using obtained knowledge through observations of single or multiple testing sessions. Given that he does not have any prior knowledge, he tries to recover the user's dataset through observation. So to have a probabilistic view of this threat, the following scenario should be considered. Each user has a learnt dataset K_i containing 12 displays' configurations. Through an authentication session, a sequence of repeated displays R_i will be randomly drawn from the K_i set, 50 times. If a display is shown at least twice, an observer can understand that it is a part of the user's learnt dataset. To find how successful an attacker might be, we need to know how many sessions are required for the attacker to acquire the knowledge of all the learnt displays K_i for a user i. To calculate this number we refer to the "double dixie cup problem" [130], which is a well-known type of the "coupon collector's problem". Given that there are n different types of coupons, the coupon collector problem finds the waiting time for a coupon collector to collect all n coupons. Each coupon is equally likely and would be randomly selected at each trial. The double dixie cup problem is an extension to the coupon collector problem and it determines the expected number of dixie cups which must be purchased in order to complete m sets of n existing different dixie cups in time t. Using the following formula we can calculate this number:

$$E_m(n) = n \cdot \int_0^\infty \left[1 - (1 - e^{-t} \sum_{k=0}^{m-1} \frac{t^k}{k!})^n \right] dt.$$

Given $n = 12$ and $m = 2$, the expected number of displays required to be exposed in order to show the entire set of user's learnt displays would be 58.04 based on the above formula. With a testing session containing 50 repeated displays in R_i (the length of R_i is 50), the attacker needs to observe 2 login sessions in order to see all learnt displays at least twice.

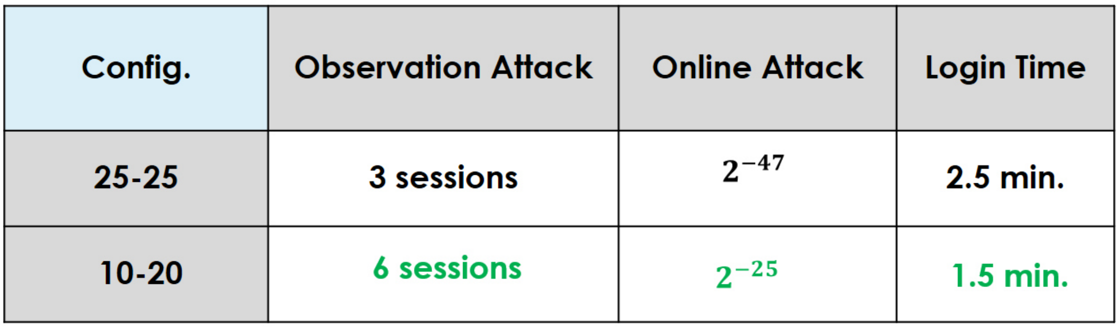
There are different amendments to the experiment configuration we can apply in order to decrease the chances of success of the observation attack while keeping the same accuracy. By exposing fewer repeated displays R_i (which we recommend have length of 10), we increase the number of sessions the attacker needs to observe (which, for 10-20 configuration is 6 testing sessions) in order to learn the user's full set of repeated displays K_i. If we were to sample from the set of learnt keys without replacement, the adversary would not learn any displays in the user's key in a single observation, but he would through observing multiple sessions and performing an intersection attack. Thus, we do not consider this an optimal enhancement. We can also increase the length of each user's learnt key. By increasing this number, we have more displays to select from and thus the attacker needs to learn more displays in order to know the user's whole set. This would result in the user needing to learn more displays; however, since the CC effect can be observed after the fourth repetition of the experiment, we may be able to decrease the number of repetitions during the training session from 15, reducing the training time despite the increased number of displays to learn. Finally, if Tacit Secrets is used for infrequently used purposes (e.g., password resets), then it may take a very long time for an attacker to observe the required number of sessions. To mitigate the chance for an attacker to learn the user's key, we can provide fewer displays in the testing session to evaluate the user's knowledge. For example, we can provide 20 repeated displays in R_i and 80 novel displays in N_i during an authentication session. Another advantage of modifying the scheme parameters is that it would also be theoretically more secure against the online attack described in Section 4.9.3. Another possible solution is to provide the user some new displays to be learnt through a testing session. Once the user i learns the display configuration through a few testing sessions, the display can be added to K_i (i.e., their key). Such a mechanism allows us to update the user's key and prevent attackers from acquiring sufficient knowledge during a series of observations.

Authentication based on RT. ***(25-25 Configuration)***. To find this configuration performance under observation attack, we need to find the expected number of sessions the attacker needs to observe to be able to determine the key. The minimum number of observations the adversary must make to learn the user's entire set of displays would be 58. Given that each login session contains 25 repeated displays in R_i, the attacker would need to observe 3 login sessions in order to be able to acquire the knowledge of the user's key.

Authentication based on RT and eye-tracking data.***(10-20 Configuration).*** For observation attack, the minimum number of observations the attacker requires to learn the user's entire set of displays would be 58. Given that each login session contains 10 repeated displays in R_i, we expect the attacker needs to observe 6 login sessions in order to acquire knowledge of the user's key.

In an extreme form of coercion, if there is no remote connection available to access the system, the attacker may also coerce the user to login to the system six times (as the number of sessions to observe and determine the user's key is six). The attacker can then masquerade as the legitimate user in order to access the physically protected room and the access user's account without any security alarm raising. Tacit Secrets might fail for this scenario; however, considering decoys in the beginning of the authentication process as discussed in Section 4.9.4, would raise an alert to the system that some suspicious interactions are happening, in which case the system will not expose the user's real key, but provide a random set of displays as the "repeated" displays. Another possible solution can be using eye-tracking data and use biometric features to detect any suspicious interaction.

Figure 4.10 shows the performance comparison of two different configurations of Tacit Secrets (i.e., basic and optimized configurations).



Config.	Observation Attack	Online Attack	Login Time
25-25	3 sessions	2^{-47}	2.5 min.
10-20	6 sessions	2^{-25}	1.5 min.

Fig. 4.10 Security performance of basic and optimal configuration of Tacit Secrets.

4.9.8 Phishing Attack

For the purpose of this discussion, we assume a faster variation of our Tacit Secrets approach (e.g., 10R-20N described in Section 4.8.4) is being used in a web environment. We consider a classical phishing attack as considered by Bonneau et al. [3]. For an attacker to launch a classical phishing attack, he/she must create a phishing site that mimics the Tacit

Secret login process (see Figure 4.11). Through this attack, the attacker attempts is to trick the user into responding to the provided challenges; that is, the Tacit Secrets displays. The attacker then records the user's reaction time on each display to find out if the display is part of the user's key. In order to gain information about whether a given challenge display d is in user i's K_i, the phishing site would need to provide d as a challenge to user i, record i's performance data for d, and compare it to i's performance data for other displays to determine whether it has better performance. If d has better performance than the majority of displays in the session, the attacker can assume $d \in K_i$. Since there are 2^{45} possible displays to challenge the user with, and each login session should only contain 30 displays, we expect it would take over $2^{45}/30 = 10^{12}$ phishing attempts on the same target user i to successfully recover i's Tacit Secret.

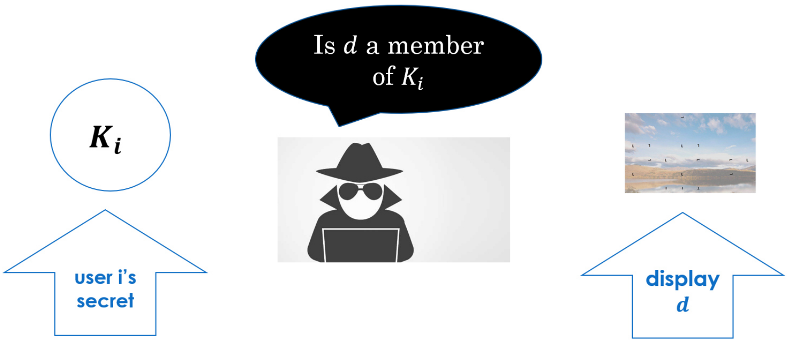


Fig. 4.11 Phishing attack for Tacit Secrets.

Tacit Secrets does not offer protection against targeted attacks including more sophisticated active man-in-the-middle, in which the attacker makes two different connection channels, one to the user who is going to prove his identity, and at the same time another connection to the verifier in order to relay the captured login secret.

4.10 Tacit Secrets Usability, Deployability, and Security Evaluation

Bonneau et al. [3] provide a comprehensive analysis of different proposed scheme for replacing replacing text-based passwords in web authentication. Focusing on 25 criteria categorize on three different groups, including usability, deployability, and security, UDS framework,they evaluate 35 different proposals. We evaluate all the identified criteria as well as two other factors for Tacit Secrets to find how it performs compared to text-based passwords. Table 4.6 shows our comparisons for Tacit Secrets with and without eye tracking data.

In terms of usability measures, Tacit Secrets outperforms passwords in different benefits. Tacit Secrets is *Memorywise-Effortless* as users do not need to memorize their assigned keys; thus, no memorability burden. Since we have theoretically shown Tacit Secrets has extremely low interference if it is used for multiple accounts (please see 4.11), we claim that it offers scalability; however, as we have not tested Tacit Secrets in real world for multiple account, we consider Tacit Secrets is potentially *Scalable-for users*. Tacit Secrets is *Quasi-Physically-Effortless* as the users need to hit the arrow keys after they find the target. Simplicity of Tacit Secrets makes it to have potential to be *Easy-to-Learn*.

The length of the training and login phase makes Tacit Secrets not *Efficient-to-Use*. Tacit Secrets is not error-prone and outperforms passwords. Tacit Secrets is *Quasi-Easy-Recovery-from-Loss* as if a user needs to reset their assigned key, they need to go through the training phase to get a new key. This feature makes Tacit Secrets worse than passwords for *Easy-Recovery-from-Loss*.

As reviewed in the related literature of CC, it remains intact in several neurological and mental disorders makes that more fascinating. It can be also used with uneducated people. So this feature may make it physically *accessible*; however, visually impaired users are not able to use Tacit Secrets. If Tacit Secrets is used without eye tracking data, it has *Negligible-*

Cost-per-User; however, incorporating eye tracking data applies cost on either the service providers or the users. Tacit Secrets is not *Server-Compatible* as it is not compatible with text-based passwords and needs it own implementation; however, it is *Browser-Compatible* as users do not have to change their client to support the scheme; however, for improved performance we need to have eye tracking device while users performing the task. It is clear that Tacit Secrets is not *Mature* widely deployed and used for actual authentication purpose. Anyone can implement or use Tacit Secrets; thus, Tacit Secrets is *Non-Proprietary*.

With eye tracking data incorporated as authentication measures for Tacit Secrets, 6 sessions are must be observed in order to find user's key. Without eye tracking data, this number decreases to 2 sessions. Although Tacit Secrets is not *Resilient-to-Physical-Observation*, it still performs better than passwords as it requires multiple observations to recover (recall Section 4.9.7). Tacit Secrets is not *Resilient-to-Internal-Observation* as a malware can detect users' interactions with the system and found out about the key; however, it still performs better than passwords as discussed in Section 4.9.2. Due to the extraordinary key space of Tacit Secrets, it is both *Resilient-to-Throttled-Guessing* and *Resilient-to-Unthrottled-Guessing*.

Due to the implicit nature of Tacit Secrets and the authentication measures that are based on the users' implicitly acquired knowledge, Tacit Secrets is *Resilient-to-Targeted-Impersonation*, *Resilient-to-Theft*, *Resilient-to-Phishing*. There is no need for *No-Trusted-Third-Party* as it does not rely on any third party. Tacit Secrets also offers the benefit of *Requiring-Explicit-Consent* since the authentication relies on a conscious consented user. Tacit Secrets is also *Unlinkable* since transactions of a user among distinct services can not be linked. Rather than the 25 benefits that are suggested in UDS framework, we also evaluate Tacit Secrets for *Resilient-to-Tailgating* and *Res-to-Key communication*. Tacit Secrets does not offer *Resilient-to-Tailgating*; however, if the user is under stress in case of coercion it might affect user to perform improperly; thus, it has the potential to offer this benefit. Moreover, the fact that the authentication key is learnt implicitly it has the benefit to be *Res-to-Key communication*.

Table 4.6 Comparing Tacit Secrets to passwords using the UDS framework [3]

.	Memorywise-Effortless	Scalable-for-Users	Nothing-to-Carry	Physically-Effortless	Easy-to-Learn	Efficient-to-Use	Infrequent-Errors	Easy-Recovery-from-Loss	Accessible	Negligible -Cost-per-User	Server-Compatible	Browser-Compatible	Mature	Non-Proprietary	Res.-to-Physical-Observation	Res.-to-Targeted-Impersonation	Res.-to-Throttled-Guessing	Res.-to-Unthrottled-Guessing	Res.-to-Internal-Observation	Res.-to-Leaks-from-Other-Verifiers	Res.-to-Phishing	Res.-to-Theft	No-Trusted-Third-Party	Requiring-Explicit-Consent	Unlinkable	Res.-to-Coerced-Tailgating	Res.-to-Coerced-Communication
Web Passwords			●		●	●	○	●	●	●	●	●	●	●		○						●	●	●	●		
With ET	● 🟩	▲	●	○ 🟩	▲	🟥	● 🟩	○ 🟥	○ 🟥	●	🟥	●	🟥	●	🟩	● 🟩	● 🟩	● 🟩	🟩	● 🟩	● 🟩	●	●	●	● 🟩	△	● 🟩
Without ET	● 🟩	▲	●	○ 🟩	▲	🟥	● 🟩	○ 🟥	○ 🟥	●	🟥	●	🟥	●	🟩	● 🟩	● 🟩	● 🟩	🟩	● 🟩	● 🟩	●	●	●	● 🟩	△	● 🟩
SISL	● 🟩	▲	●		●	🟥	🟥	🟥	○ 🟥	●	🟥	●	🟥	●	🟩	● 🟩	● 🟩	🟩	🟩	● 🟩	● 🟩	●	●	●	●	△	● 🟩
Mooney Auth	● 🟩	▲	●		▲	🟥	● 🟩	○ 🟥	○ 🟥	●	🟥	●	🟥	●		● 🟩			🟩	● 🟩		●	●	●	●		

● – offers the benefit, ○ – almost offers the benefit, no circle – does not offer the benefit, ▲ – potential to have the benefit , △ – potential to almost offer the benefit, 🟩 – better than passwords, 🟥 – worse than passwords

4.11 Discussion

There are different amendments to the experiment configuration we can apply in order to decrease the chances of success of the observation attack while keeping the same accuracy. By exposing fewer repeated displays R_i, we increase the number of sessions the attacker needs to observe (e.g., for 10-20 configuration, it is 6 login sessions).

We can also increase the length of each user's learnt key. By increasing this number, we have more displays to select from and thus the attacker needs to learn more displays in order to know the user's whole set. This would result in the user needing to learn more displays; however, since the CC effect can be observed after the fourth block in training, we may be able to decrease the number of repetitions during the training session from 15. Another possibility is to provide the user some new displays to be learnt during each login session. Once user *i* learns the display configuration through a few testing sessions, the display can be added to K_i (i.e., their key). Such a mechanism may allow us to update the user's key and prevent attackers from acquiring sufficient knowledge during a series of observations. Finally, we note that if direct implicit learning-based authentication tokens, Tacit Secrets, is infrequently used (e.g., for password resets), then it may take a very long time for an attacker to observe the required number of sessions.

In this section we first provide a summary of our results. We then discuss Tacit Secrets use case and then compare Tacit Secrets with the previously proposed implicit learning-based authentication scheme. We then discuss the interference of Tacit Secrets between multiple systems. We also evaluate Tacit Secret performance against phishing attack.

4.11.1 Summary of Results

In this chapter, I introduced the proposed direct implicit learning-based authentication tokens, "Tacit Secrets". Using *contextual cueing* as a cognitive paradigm, through a lab study, I was able to elicit subjects' implicit memory in order to train them on a system-assigned authentication key. The assigned keys were in form of a set of *contexts*, 2-dimensional spatial configuration of irrelevant objects (aka. *distractors* - L letters) in which a target (T letter) is presented. The participants were trained on their assigned keys and if they have previously seen the context and learnt the position of the items on that, they had better performance in finding the target whereas for novel contexts they had worse performance. The improved performance was due to the knowledge that they acquired implicitly and without their conscious during the training session. Thus, I found that such knowledge has potentials to be used for authentication. To verify feasibility of Tacit Secrets for authentication, I first needed to evaluate if I can gage users' knowledge on the trained key. I used a single metric, *reaction time* (RT), and I was able to verify the acquired knowledge is accessible and can be measured for authentication purposes.

After I found promising results through the initial analysis, in order to further improve the results of the proposed approach, I incorporated some ocular parameters as the second layer of authentication metric. Using eye tracking data, I could improve the approach performance. The results showed 92.86% of the participants could successfully login to their accounts seven days after the were trained on their assigned keys. I also evaluated different security metrics for Tacit Secrets approach and examined different configuration of it. The feasibility study also indicated that the approach has strong security properties: resistance to brute-force attacks, online attacks, classical phishing attacks, some coercion attacks, and targeted impersonation attacks.

4.11.2 Tacit Secret Use Case

Tacit Secrets could be used for any system requiring the strong security guarantees offered by system-assigned passwords. However, our current design has long login times that limit its practicality. We believe the current design we studied would still be useful in some environments with high security requirements, e.g., unlocking a critical system configuration terminal, unlocking a high-security vault or room.

Our version that incorporates eye-tracking indicators is expected to have login times on the order of 1.5 minutes, and thus might also be acceptable for infrequently accessed web or financial accounts. If future work shows the implicit memory effect lasts for longer time periods, it may also be useful for fallback authentication.

4.11.3 Comparison to Previous Method

We found Tacit Secrets has a much better performance than a previously proposed coercion-resistant scheme, SISL [31]. SISL is the most widely used for coercion resistant.

The authentication process in SISL is based on the users' performance (the percentage of the correct responses and response time) on the learnt sequence versus random ones. This data can be used to prevent the same coercion attacks as Tacit Secrets; however, only 71%, 47%, and 62% of participants could successfully authenticate using this method immediately, 1 week, and 2 weeks later respectively. SISL's first experiment aimed to confirm the existence of implicit learning through an authentication session immediately after training. Their second experiment had two groups of participants: the first group did the SISL task one week after training. The second group did the SISL task two weeks after training, where the length of the testing session was doubled (from 5-6 minutes to 10-12 minutes) to see if this change could affect their performance. For this second group of participants, 62% exhibited better performance on the trained sequences. The improvement in the authentication success rate (from 47% to 62%) was due to doubled length of the testing session for the 2-week delay group (from approx. 5-6 minutes to approx. 10-12 minutes). This change resulted in better performance and more sensitivity of the subjects to their implicitly acquired knowledge.

Our results showed that Tacit Secrets offers substantial improvements over SISL, increasing success rates from 71% to 100% and 47% to 96%, immediately and one week later respectively, reducing training times from 30-45 to 14.5 minutes, and reducing the login times from 6-12 minutes to 1.8-1.5 minutes for the immediate and 1-week delay authentication sessions respectively.

4.11.4 Interference Between Multiple Systems

Although the key space for Tacit Secrets is large, there might be some possibility for interference between the assigned keys and novel displays of different systems that use Tacit Secrets. This scenario would occur when the novel displays (randomly generated by system A), happen to be part of the user's key for another system (e.g., system B). Given that the possible number of displays generated by Tacit Secrets is 2^{49}, and each system has 12 learnt displays (also randomly assigned), even if we assume there are 100 systems using Tacit Secrets, the probability of such an interference would be 4.22×10^{-11} (see Figure 4.12).

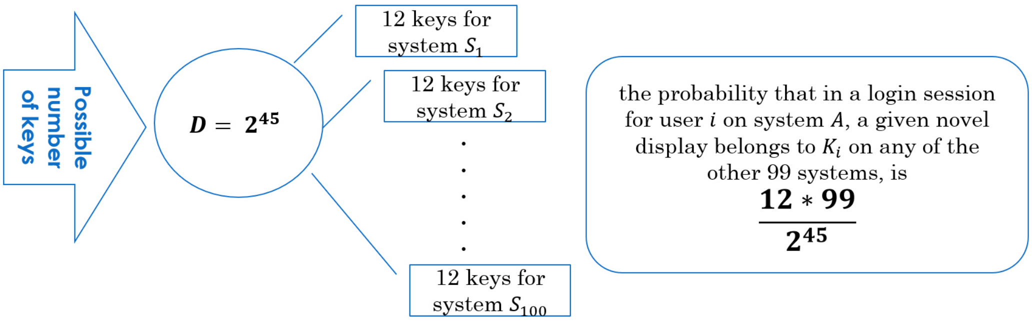

Possible number of keys
$D = 2^{45}$
12 keys for system S_1
12 keys for system S_2
12 keys for system S_{100}
the probability that in a login session for user i on system A, a given novel display belongs to K_i on any of the other 99 systems, is
$\frac{12 * 99}{2^{45}}$

Fig. 4.12 Interference between multiple Tacit Secrets scenarios.

4.12 Limitations

Most experiment-based studies have limitations and ours was no exception. As discussed in Section 4.11, the proposed system is not intended to be used for everyday authentication (e.g., e-mail accounts, e-banking). Through our experiment we found some evidence for a couple of subjects (i.e., 6%) that had difficulty focusing on the task, leading to unacceptable performance and learning for the second and third testing sessions. These subjects were unable to find the target during the exposure of the displays and they had a high rate of no-response or wrong-response answers. However, we found through our analysis that a much shorter session is possible when eye-tracking data is incorporated; we expect that this shorter task duration might improve focus for these few users.

Given that the CC task facilitates implicit learning, Tacit Secrets can be considered an authentication mechanism that has no explicit memorization burden on users; however, it is possible that implicitly learnt passwords do impose a cognitive load we are not aware of. Guaging such cognitive loads is out of the scope of our work.

4.13 Ecological Validity

Recent technological improvements have been facilitated data collection process for researchers. It helps them to process large quantities of data in a speedy way. However, it raises the question if the behavioral sciences, including research on human computer interactions, have considered issues related to ecological validity related to design of studies as well as results. Several factors may affect the ecological validity and generalizability of our results.

For direct implicit learning-based authentication approach, the tasks were performed through in-lab study where the participants were involved in a controlled lab environment, provided with brief instruction (verbal and visual). The experiment was equipped with an eye tracking device that they needed to go through a simple calibration process. Since ecological validity entails how findings can reflect the behaviour that occurs in more naturalistic settings, conducting a study on campus will restrict the participants to of same age range as well as having some level of education. Although they represent a large segment of the Internet users, any attempt to generalize our results should be done with caution as all of our participants are undergraduate with some level of education. Thus, it might affect generalizability of the results.

Another factor which needs to be considered is that during the study participants may be nervous, ill at ease and is unlikely to perform in the same way as they would in a their own environment of choice. It is worth noting that for all studies there is a trade-off between experimental control and ecological validity. Conducting in-lab study will provide more control for researchers while decreasing the ecological validity. The more control researchers exert in a study, the less ecological validity and thus less generalization.

4.14 Conclusions

We proposed a new authentication scheme we call Tacit Secrets, whereby a user implicitly learns a random key that is resistant to coercion attacks. We conducted an experiment to demonstrate that Tacit Secrets can provide an implicitly learnt key for authentication purposes. Our findings indicate that Tacit Secrets has a significantly higher success rate of authentication compared to previous work using implicit learning. It also has a significantly reduced training and login time. We performed additional security analyses to better quantify the security offered by this scheme. Our findings suggest that authentication using CC is possible and viable. Future work is needed to determine whether training and testing times can be even further reduced than our analyses suggest. Determining the optimum number of repetitions and frequency of training would however require considerably more experimentation. For future work, we are also interested in exploring other enhancements such as how the uniqueness of the movement of the eye as a behavioral biometric can result in a shorter Tacit Secrets login, yet maintain accurate identification of users.

Our work suggests that directly using implicitly learnt secrets in authentication can be a viable approach in some contexts. Future work also includes exploring whether implicitly learnt information could be used indirectly to facilitate memorization of authentication secrets.

4.15 Future Work

The design of the proposed approach is based upon the previous works related to the contextual cueing paradigm. To be consistent with those studies, for the training session, we considered 15 blocks containing 16 trials. Although the learning effect is detectable after the fourth block [119, 120], I stick to the same number of blocks as previous CC studies. So for the sake of consistency with the previous CC studies, for the training session, I considered 15 blocks containing 16 trials (taking approx. 14.5 minutes). However, this number might be further reduced to produce lower training times. We leave it for future work to investigate if the training session can be further shortened while the learning is still effective and durable.

Another issue of the proposed method that needs to be discussed is the fading effect of the learnt key. Based on our analysis, the difference between the average RT for the novel and repeated displays appears to have decreased over the course of the experiment. This might imply that there is some fading of the CC effect over time. To mitigate the effects of implicit knowledge fading, a periodic training session could be seamlessly inserted during regular authentication sessions to make sure the displays used for authentication get continuously renewed as needed. But this would require further analysis. The retraining process can be done through either learning new displays during multiple testing sessions which can update the user's dataset partially, or it can be done through a new training session which updates the entire user's dataset and adds the previously learnt displays. Finally, since the knowledge acquired through CC lasts for delays of at least six weeks [29, 30], it would be interesting to determine whether it exists for longer durations to evaluate its suitability for fallback authentication.

Chapter 5

Implicitly Reinforced Passphrases

As per direct implicit learning-based authentication secrets, we found evidence confirming the robustness of contextual cueing as an implicit learning mechanism to be used for authentication. To further explore how this mechanism (i.e., CC) can be used to enhance user's memorability of system-assigned secrets, we designed and implemented an approach to use it for reinforcing user's explicit memory. The idea is to use contextual cueing and semantic priming to leverage implicit learning in order to reinforce the memorability of system-assigned passphrases. We call the proposed approach "Implicitly Reinforced Passphrases". As discussed in Section 2.4, semantic priming is a form of priming in which the prime is semantically related to a subsequent test word [131]. Having a fixed set of objects which are semantically related aids semantic priming.

The remainder of this chapter is organized as follows: I explain the system design, more details about how the experiment is set up in terms of the provided training mechanism, user task in each part of the experiment, and how the experiment is organized for the users. I also provide more information about the participant recruitment process as well as how I analyze the collected data. This chapter continues with more security and usability evaluation. I wrap up the chapter with related discussion and conclusion and future directions.

5.1 Implicitly Reinforced Passphrases Mechanism

Most people find passphrases more memorable than passwords containing different types of characters. Such sentences are more memorable when they have a sentence structure in a natural language. It is much simpler to recall a sentence which means something to the user, than passphrases with no structure and meaningless to the user which have been generated by a machine [60].

5.2 System Design

Our proposed approach uses two implicit learning-based paradigms indirectly and trains users on system-assigned passphrases. The goal is to facilitate the memorization process of system-assigned passphrases and make it easier to recall them later. The essence of the idea is to provide a short training phase during enrollment to invoke implicit learning, then subsequent logins proceed normally without additional training. The training is enabled by a combination of two implicit learning based cognitive paradigms, CC and SP. Users are assigned a 4-word passphrase and each word is presented in a display surrounded by 31 semantically related words. CC is defined through a 2-dimensional spatial configuration of irrelevant objects (aka. distractors) in which a target is presented. CC relies on distractor positions to provide spatial cues for the location of a target. The entire spatial configuration is shown on a display, for a fixed period of time [45]. We involved CC in the proposed approach by creating word displays, which have spatial configurations of words preserved on them. These four displays are shown to the users repeatedly. Each display contains a word of the passphrase and the user task is to find a word (i.e, passphrase word) with different font. To decide how many repetitions are required for a stable training, we referred to the previous studies, confirming that CC knowledge is accessible after four repetitions [119, 120]. Through several rounds of pilot testing, we found five repetitions provides sufficient training in order to learn the passphrase. In terms of the number of words displayed on each display, 32 words, we also tested different numbers of words on 6×11 displays during pilot studies. We found increasing the number words per display prevents users from properly processing the relationship between the words and could cause distraction. We found 32 words placed in a 6×11 matrix, is a number which can be processed for both the location of the items as well as the semantic relation between the words. These four displays are shown five times for five seconds each. If the user does not find the target word within five seconds the next context appears. We randomly selected each context's words from a dataset of 923 different words.

Given that cues are provided for the login session, for a successful online attack, the number of guesses the attacker needs to make is $4 \times 2^5 = 2^{20}$ (for a 4-word passphrase, each presented on a display of $2^5 = 32$ words). We decided on a 4-word passphrase as it provides a keyspace of 2^{20} ($\gtrapprox 10^6$) which has negligible risk of online attack [129]. This has been the value cited for online attack resistance in many subsequent security solutions (e.g., [10, 132]). Florêncio et al. [129] discuss strength beyond 2^{20}, concluding that keyspaces between 2^{20} and 2^{47} fall in the "don't care region" or the online-offline chasm, whereby little is gained in terms of security, but the cost to usability can be noteworthy. Thus, we designed our system to have a 2^{20} keyspace.

We also included a condition containing SP only. The SP condition is employed by providing 32 words that are semantically related. The four displays are exposed to the users with no repetition or preserved locations of the words. The user task is to find a word that has different font than others (this word is one of their assigned passphrase words). The provided displays are intended to help users to make mental associations (using their semantic memory) for these words. Studies of SP have observed that a response to a target is faster when it is preceded by semantically related primes [55–57]. The priming occurs because the provided primes activate the viewer's mental encoding of related words or concepts, facilitating their later processing or recognition. The goal of this design is to encourage such mental relations to prime them to recall the assigned passphrase later.

We used the woverd2vec model [133] which provides an efficient implementation of the continuous bag-of-words for computing vector representations of words. The word2vec tool takes a text corpus as input and produces the word vectors as output. It first makes a vocabulary from the training text data and then learns a vector representation of the words. These representations can be subsequently used in many natural language processing applications. By finding the distance of word pairs, using a distance tool [133], we can find the similarities between the words. Using this tool, given the similarities between the words (in a range of -1 to 1), we selected a set 32 of words with equal similarities (between 0.4 to 1) from each other. If we only consider the distance of each word from target word, then the target word can be easily guessed by the attacker as all words have a relation with that word and not necessarily each other; however, making this relation between all words on the display prevents the target word from being computable. For our study we generated 10 passphrases, so we made a dataset of 40 word displays given the above limitations. The 40 words were selected from a dataset of 923 distinct words [133].

We also included another condition, including the CC effect solely. For this condition, users are provided with 4 displays containing some words with no semantic relations. Figure 5.1 shows a sample display for the training session of CC-SP condition. After the training, through three different sessions, we examine users to see if they can successfully recall their assigned passphrases.

As shown on Figure 5.1, the user's task is to find passphrase words and click on it. Such a design is expected to reduce the number of errors associated with passphrase input. It can improve common issues such as forgetting word order, typos, and extra time to input many more characters.

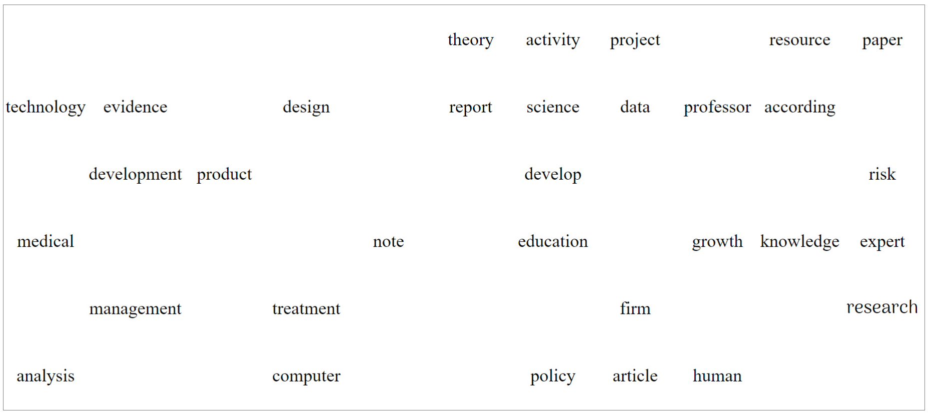


Fig. 5.1 Sample CC-SP display for Implicitly Reinforced Passphrases Experiment. The target word is ‘research’.

5.3 Study Design

On a high level, our system trains users to implicitly learn a secret set of contexts, which becomes their system-assigned passphrase. Our work aims to determine whether by involving some IL mechanisms, we can improve, or reinforce, user’s memory for system-assigned passphrases. To examine this hypothesis, we designed an experiment through which users are provided with a training phase, designed to evoke implicit learning, for system-assigned passphrases. The training phase is performed through the combination/single usage of two different implicit learning processes; that is, CC and SP.

5.3.1 Hypotheses

Our high-level research question is: Can IL improve (or reinforce) memorability of system-assigned passphrases? Using IL mechanisms, we expect the provided training would result in improved memorability compared to the other conditions which do not involve any training. The following statements articulate our hypothesis:

$H_{memorability}$: There will be significantly greater memorability in IL-based trained passphrases compared to the control conditions. To test this hypothesis, the following hypotheses should be answered:

- $H_{memorability-recall}$: There will be a significant improvement in the number of users who correctly recalled their assigned passphrase words.
- $H_{memorability-record}$: There will be a significant improvement in mean number of users who recorded their passphrase.

$H_{usability}$: There will be significantly greater usability in IL-based trained passphrases compared to the control conditions. To answer the above hypothesis, the following hypotheses should be answered for IL-trained passphrases vs. the appropriate control conditions (see next section for a discussion of which control is used for each IL condition).

- $H_{usability-logintime}$: There will be a significant improvement in time required to login.
- $H_{usability-susscore}$: There will be a significant improvement in user sentiment in IL-based trained passphrases compared to the control conditions.

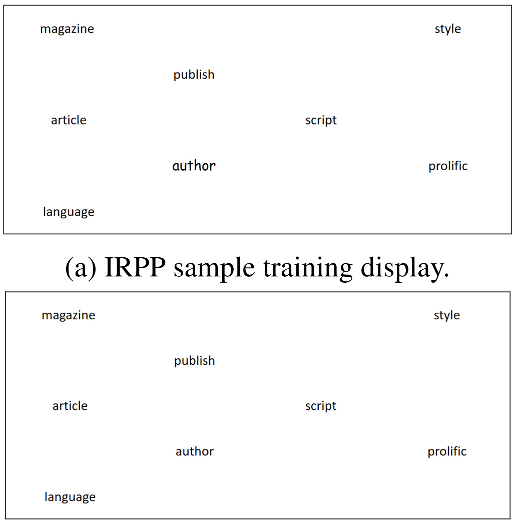
$H_{login-nocue}$: The provided training is effective enough to help users recall their assigned passphrase without providing cues in the login session.

5.3.2 Study Conditions

Given the high-level research question (i.e., can IL improve memorability of system-assigned passphrases?), our specific approach to answering this question is explained below. In particular, we examine the use of specific processes known to invoke IL. Thus, our research examines the following more specific question:

Can we improve memorability of system-assigned passphrases using a combination of CC and SP for training users on their assigned secrets? To answer this question, we provide the following conditions:

Condition 1 (CC-SP). The first experimental condition provides participants with a training session that presents semantically related words in repetitive-stable contexts (i.e., similar to the contexts used in CC). This condition helps us to determine if the combination of CC and SP can improve passphrase memorability (see Figure 5.2a). For the training session, each word of the assigned passphrase is presented on a context containing 31 other semantically related words. Each user is shown four contexts (4-word passphrase). The user task is to find a word with different font than other words (i.e., the passphrase word) and click on that. The four contexts are repeatedly shown to the user five times. As the repetition of the task comes from CC, previous works on CC showed learning occurs after 4 repetitions. Thus we decided to choose a the number based on the previous findings. Moreover, we ran multiple pilot studies testing different numbers for repetitions. We found five repetitions sufficient to stabilize the knowledge. For participants in this group, a login session is set up in a way that they will be provided with the same contexts as their training session (to be used as cues). The only difference is that the target word is no longer in different font (see Figure 5.2b).



(a) IRPP sample training display.

(b) IRPP sample login display.

Fig. 5.2 Simplified CC-SP condition context for training and login. Please note that in our actual experiment each context contains a target word (passphrase word) surrounded by 31 distractor words (see Appendix B.3 for examples showing full displays given in our experiment).

Condition 2 (Basic Passphrase Control). Participants in this group are assigned a passphrase with no specific training involved. They are given unlimited time to memorize their assigned words. This group's participants are later asked to recall their assigned passphrase by typing the four words in four text boxes. Comparing this with Condition 1 (CC-SP) can tell us whether our CC-SP approach has been effective in improving system-assigned passphrase memorability. The remaining conditions are used to identify how effective each IL technique has been in memorability improvement.

Condition 3 (CC). This condition is the same as Condition 1 (CC-SP), but there are no semantic relations between the words. In other words, the contexts contain unrelated words. Contexts shown to the participants in this group are as shown in Figure 5.2a; however words are random with no semantic relations. We provide the previously seen contexts as cues for the login sessions. Comparing this condition with Condition 1 (CC-SP) will indicate whether any improvement offered by CC-SP would also be offered by CC alone.

Condition 4 (SP). This condition is the same as Condition 1 (CC-SP), but there is no repetition of the displays during training, and no stable locations for the words. Since there is no repetition and no stable locations, there is no CC in the training. The 32 words are randomly placed in a display with 66 possible positions. We provide these words (in shuffled locations within the context) as cues for the login sessions. In training, each display of 32 words is shown once, and the user task is to find the word with different font and click on it. This condition is included to see if users have higher recall rates when semantically related words are provided for their login sessions. Comparing this condition with Condition 1 (CC-SP) will indicate whether any improvement offered by CC-SP would also be offered by SP alone.

In the event of any memorability improvement for system-assigned passphrases while using our IL-based interfaces, is it due to our special IL-based training or it is just due to repetition, or recognition, or both?

To answer this question, the following control conditions need to be evaluated and compared with the previous conditions.

Condition 5 (Repetition). This condition is to help us answer: Are improvements using IL-based interfaces due to repetitions in the training phase and recognition in the login phase? The condition is the same as Condition 1 (CC-SP) and 3 (CC) in terms of the displays (each containing one passphrase word) having the same number of repetitions; however, there is neither semantic relation between words, nor stable location of the words. For this condition, users are provided four consecutive contexts where each contains a passphrase word which is surrounded by 31 random words (i.e., no semantic relation exists). These four contexts are repeatedly shown to the users five times; however, in contrast to CC or CC-SP, there is no stability in the location of the words. As in all other conditions (except Condition 2), users are supposed to find a word which has different font. For the login session, the users are provided with the displays which have no preserved locations for the words. Comparing this condition with the CC condition indicates whether the combination of repetition and recognition can be the source for improved memorability rather than CC.

Condition 6 (Recognition). This condition is to help us answer: Is the effectiveness of training due to recognition, or our special IL-based interface? The condition is the same as Condition 5 (Repetition); however, there is no repetition involved for the training. For this condition, users are provided with four consecutive displays where each contains a passphrase word surrounded by 31 random words (i.e., no semantic relation exists). In the training phase, for each of the four contexts, users are tasked with finding a word which has different font than the other words. Each display contains one passphrase word, and is shown only once. For the login, the users are provided with the displays to see if they can recognize their passphrase words. Note that for each login, each display has a random configuration of the same 32 words. Comparing this condition with SP indicates if recognition is the reason for memorability success rather than SP. Comparing this condition with Condition 5 (Repetition) will determine whether repetition is the cause of improved memorability rather than recognition. Table 5.1 indicates how each condition includes CC and/or SP.

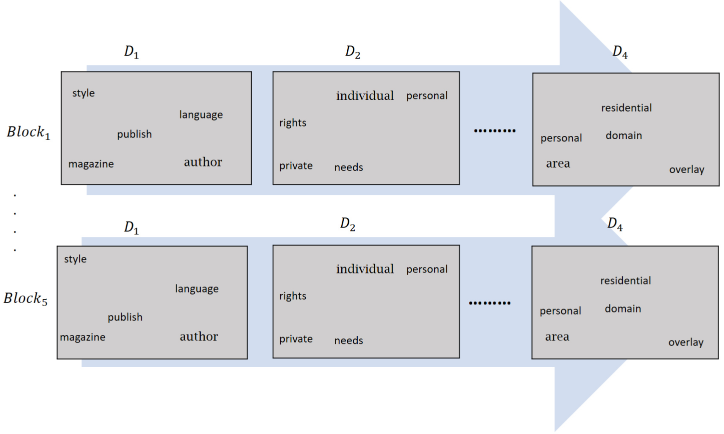


Fig. 5.3 An example of displays arrangement during the training sessions.

Table 5.1 Each condition specification. Some of the conditions include fixed location of the words, repetition, exposure time, and/or the words with semantic relation. CC includes fixed locations, exposure time, and repetition.

Condition	Semantic Relation	Fixed location	Repetition	Exposure Time	Login Cues
CC-SP	✓	✓	✓	✓	✓
Control	-	-	-	-	-
CC	-	✓	✓	✓	✓
SP	✓	-	-	-	✓
Repetition	-	-	✓	✓	✓
Recognition	-	-	-	-	✓
CC-SP w/o Cues	✓	✓	✓	✓	-

Can we improve security of the proposed scheme by not exposing any cues for the login session?

To answer this question, we examine the following condition.

Condition 7 (CC-SP w/o Cue). This condition is the same as Condition 1 (CC-SP); however, for the participants in this condition, the displays are not provided for the login session. Participants need to input their four assigned passphrase words in four text boxes. Comparing this condition with Condition 1 (CC-SP) allows us to find out whether for higher recall rates, there is a need for cues to be provided for the login session. If participants in this group have higher or equal recall rates compared to the participants in Condition 1 (CC-SP), we can conclude that there is no need for further cues in the login session which enhances security as the attacker cannot observe a session and narrow down the possibilities of what a user's passphrase might be. In this variation of the system, the passphrases are arguably secure against both offline and online attacks. We can also compare to Control to see if the training phase alone can improve memorability of the assigned passphrase.

5.3.3 User Studies

We first tested our indirect implicit learning-based authentication secrets approach through a web application pilot study where we asked 10 participants to test our designed web application and provide us with their feedback. Using their feedback, we were able to further improve the design of our system. Their comments helped us to modify the instructions that participants were provided.

We used MTurk crowdsourcing service to evaluate our conditions. All our user studies were reviewed and approved by our Research Ethics Board. We first recruited 100 participants through MTurk to evaluate the feasibility of our proposed scheme. Of the 100 participants, 50 were assigned the control condition and the remaining 50 CC-SP. As we were using semantic relations of English words, we needed our participants to know English well; thus, we limited the participants to be from English-speaking countries. The first phase of our online study confirmed the effectiveness of CC-SP for memorability improvements for the users. Thus, we started the second phase of our study and recruited another 780 participants and randomly assigned them one of our study conditions. We compensated them 50¢ for completing the first session of the study and two additional 25¢ for completing the second and third sessions.

In the first session of our study, we provided the participants with the same statement as Shay et al. [64] used in their study. “Imagine that your main email service provider has been attacked and that because of the attack, your email service provider is also changing its password rules. Instead of choosing your own password, you will be assigned a 4-word passphrase.” We asked them to: “Please take the time you need to memorize your passphrase words (and their order).”

For the first session, once each participant signed up for the study and consented participation, he/she was randomly assigned one of our six study conditions. The participant was then assigned a 4-word passphrase. Depending on the condition, the participant was provided with either no training (basic control) or one of our five designed training sessions. Participants in the Control condition were provided with the following instructions through three consecutive web pages: (1) “Below you can see a sample that shows the four words of an assigned passphrase.”, (2) “Next you will be shown the 4 words of your passphrase. Please take the time you need to memorize your passphrase words (and their order).”, (3)“The training session will begin next. After the training, you will be asked to login with your passphrase.”. For participants in the SP, and Recognition conditions wherein no repetition was involved, the following instructions were provided: (1) “Each word of your passphrase will be presented in a grid of words. This word is shown in different font. Below you can see a sample that has the word with a different font circled in red. Note that in your task, these words will not be circled in red as in this sample.”, (2) “When you find the word with different font, click on it. Notice that the table border provides you the feedback based on your response. Practice on the display below.”, (3) “The training session will begin next.After the training, you will be asked to login with your passphrase.”. For participants in the CC-SP, CC, Repetition, and CC-SP w/o Cue the following instructions were provided: (1)“Each word of your passphrase will be presented in a grid of words. This word is shown in different font. There is a time limit of five seconds for each arrangement of words. Below you can see a sample that has the word with different font circled in red. Note that in your task, these words will not be circled in red as in this sample.", (2)"When you find the word with different font, click on it. Notice that the table border provides you the feedback based on your response. Practice on the display below.", (3)"The training session will begin next. After the training, you will be asked to login with your passphrase.".

Before starting training session, a sample display was provided for the participants to practice the task before going through training.

After training, participants were asked to login. For all login sessions, for all sessions in the study, participants needed to recall their passphrase within maximum five attempts. If they failed remembering after five attempts, their passphrase was shown to them and they were asked to memorize it. For this session, participants in the Control, and CC-SP w/o Cue conditions wherein no cue was provided for the participants, the following instructions were provided: "You will be provided with 4 text boxes to enter 4 words of your passphrase. You can have up to 5 attempts in order to input your passphrase successfully. Below you can see a sample input page.". The provided instruction for other conditions was as follows: "You will be provided with 4 displays, each containing 32 words. Your task is to: (1) Find the word of your previously assigned passphrase words. (2) When you find the word, click on it. (3) Once you click on the word, the next display appears. (4) If you don't find the correct words, you are given up to 5 attempts to find correct words. Below you can see a sample display.".

We then asked the participants to return after 24-48 hours, and again one week after their first session in order to complete the second and third sessions respectively. They also received an email notification in order to remind them about the follow-up sessions. In the second session, participants were asked to recall their passphrase. The third session was identical to the second with an additional questionnaire which was provided at the end of the login task.

5.3.4 Statistical Testing

Using a significance level of α = .05, for each comparison, we first ran an omnibus test across all conditions. For non-normal distribution we used Kruskal-Wallis. We used χ^2 on categorical (e.g., number of attempts needed for successful login). If the omnibus tests showed significance, we performed selected pairwise tests of interest. We also performed the Holm-Bonferroni correction (indicated HC) for multiple-comparison correction. This test performs an adjustment made to p-values when several dependent or independent statistical tests are being performed simultaneously on a single data set.

5.4 Results

In this section, we present our proposed approach results. We first provide some demographics of the participants. We then provide some information about the participation and drop-out rates across all experimental conditions. Finally, we describe the data regarding participants in each condition who recorded their passphrases, recalled their passphrase, forgot their passphrase, login times, and exit survey results.

5.4.1 Participants

1003 participants initially signed up for our study, 880 of whom finished the first part. Of the participants who finished the first part, 476 and 430 finished the second and third part of the study respectively. 52% of our participants were male and 48% were female. For education levels, 5% had high school or equivalent, 71% had a college or university degree, 18% master degree, and 4% doctoral degree. 41% of the participants were aged between 26-35 and 31% between 36-50. 97% of the participants had English as their first language.

5.4.2 Study Dropouts

We ran the online study in two different phases. During the first phase the we recruited participants for the CC-SP, Control, CC, SP, Repetition, and Recognition. This allowed us to find out how each condition performs. After we found CC-SP outperforms other conditions, we ran our second phase of the experiment for the CC-SP w/o Cue condition. This allowed us to came to a conclusion if removing the cues from the login session can affect authentication success rates.

Of 1003 participants who started our study, 880 finished the first part; 576 participants returned within 24 to 48 hours of receiving our email invitation and completed the second part of the study, and 430 participants completed the third part of our study. These statistics, broken down by condition, are shown in Table 5.2. As shown on the table the return rate for the second phased of our study is higher than phase one. This could be due to the less number of participants that we needed to hire (as we had one condition versus 6 conditions). This, those participants who were working on MTurk actively could have signed up for the HIT and as a result they were more likely to come back for the following sessions.

Condition	Started	S1	S2	S3
CC-SP	155	84%	53%	51%
Control	149	88%	52%	48%
CC	137	93%	58%	50%
SP	139	91%	54%	50%
Repetition	150	88%	54%	42%
Recognition	163	81%	50%	47%
CC-SP w/o Cue	110	91%	71%	64%

Table 5.2 The number of participants who signed up for the study in each condition, and the percentage who continued all three sessions (i.e., Session 1, Session 2, and Session 3).

5.4.3 Storage

Our application captured those participants who either did a copy-paste action (for the control condition) or screenshot while they were performing the task. For those participants who finished all three sessions, through the exit questionnaire we asked them if they have recorded their assigned passphrase. Table 5.3 indicates the number of participants in each condition who recorded their passphrase. Note that in this table we did not double count those who mentioned in the questionnaire that have stored their passphrase and also our system detected their copy-paste action.

Condition	Copy-Paste	Screenshot	Record	Total Percentage
CC-SP	0	2	9	7%
Control	6	8	34	26%
CC	0	2	12	9%
SP	0	0	12	9%
Repetition	0	1	20	15%
Recognition	0	2	19	14%
CC-SP w/o Cue	3	0	8	7%
Total	9	15	114	

Table 5.3 The number of participants who recorded their assigned passphrase.

The table indicates the number of the participants who either mentioned in the questionnaire that they recorded their passphrase or the system caught their copy-paste or screenshot actions. The last column of the table indicates the total percentage of the participants in each group who have performed any type of storage. We hypothesize there will be a significant improvement in mean number of users who recorded their passphrase. The null hypothesis that we claim for the purpose of dependency between the condition and storing bahaviour, assumes that there is no association between the condition and storage behaviour. Running χ^2 showed a significant difference in recording behaviour of the CC-SP condition compared to the Control condition ($\chi^2 = 17.96, p < .001$) which rejects the null hypothesis and confirms the participants in CC-SP did not need to record their passphrase while for the control condition, more participants had recorded their passphrase.

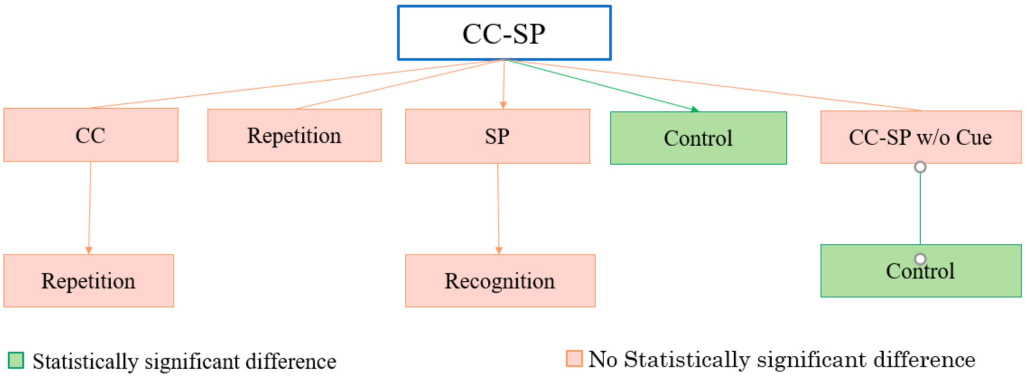

CC-SP
CC
Repetition
SP
Control
CC-SP w/o Cue
Repetition
Recognition
Control
🟩 Statistically significant difference
🟥 No Statistically significant difference

Fig. 5.4 Pairwise comparison of the experimental conditions for authentication success rate for the third login session. The green rectangles show significant difference whereas the orange ones indicate no statistically significant difference.

Conditions	*p-value*	HC
CC-SP and Control	< .001	0.006
CC-SP and CC	0.8	0.012
CC-SP and SP	0.8	0.012
CC-SP and Repetition	0.05	0.007
CC-SP and CC-SP w/o Cue	0.9	0.016
CC and Repetition	0.1	0.008
SP and Recognition	0.2	0.01
Control and CC-SP w/o Cue	< .001	0.006

Table 5.4 The results of Chi-Square for the pairwise comparison for the storage behaviour for the experimental conditions. Holm-Bonferroni Correction (HC) was applied on the set of 8 pairwise tests for the S3 storage behaviour. HC column shows the updated alpha value for achieving significance. The highlighted rows show the conditions with statistical significant difference.

5.4.4 Recall Rates

We asked our participants to recall their passphrase three different times, including immediately after training, 24-48 hours later, and 7-8 days after training. Participants who were not able to recall their passphrase after five attempts are considered as having forgotten their passphrase and were shown the passphrase on the screen.

First Session

For an immediate recall test, most participants successfully recalled their passphrase. Table 5.5 shows the successful recall on both first entry and those who needed more attempts to recall. As per $H_{memorability-recall}$, we hypothesized there will be significantly greater memorability in IL-based trained passphrases compared to the control condition. The null hypothesis that we claim for the purpose of dependency between the condition and success rate, assumes that there is no association between the condition and login success rates. As shown on the table, the CC-SP condition outperformed the others, having the highest total success rate and lowest average number of attempts in order to successfully login. Running χ^2 indicated a significant difference across conditions ($\chi^2 = 26.20, p < .001$). This will reject the null hypotheses and indicates an association between the group and login success rates.

		Success first attempt	More attempts	Avg login	Total success
Conditions	CC-SP	96.92%	0.77%	8.14	97.69%
	Control	78.63%	6.11%	14.33	84.73%
	CC	91.41%	2.34%	9.08	93.75%
	SP	85.83%	3.94%	12.33	89.76%
	Repetition	85.61%	5.3%	19.6	90.91%
	Recognition	74.24%	6.06%	22.09	80.30%
	CC-SP w/o Cue	80%	9%	11.23	89%

Table 5.5 First login session total success rate percentages, the percentages of those who needed more attempts to login, and average login duration (in seconds) for each condition.

Second Session

We sent our participants a notification email 24 hours after the first session and asked them to login to our web interface by recalling their assigned passphrase. The participants who came back within 24-48 hours were able to access our system. Running χ^2, indicated a significant difference across conditions ($\chi^2 = 14.05, p = .01$). Table 5.6 indicates the success rates across all experimental conditions. CC-SP remained the condition with the highest total success rate and lowest login time.

		Success first attempt	More attempts	Avg login	Total success
Conditions	CC-SP	87.8%	3.66%	10.76	91.46%
	Control	65.38%	8.97%	25.43	74.36%
	CC	81.01%	6.33%	15.32	87.34%
	SP	70.67%	9.33%	21.32	80.00%
	Repetition	72.84%	9.88%	27.07	82.72%
	Recognition	67.90%	4.94%	30.39	72.84%
	CC-SP w/o Cue	74.36%	6.41%	22.09	80.77%

Table 5.6 Second login session total success rate percentages, the percentages of those who needed more attempts to login, and average login duration (in seconds) for each condition.

Third Session

The third part of our study was 7-8 days after the first session. The participants who had completed the first two sessions were qualified to perform this task. Running χ^2, indicated a significant difference across conditions ($\chi^2 = 22.76, p < .001$). CC-SP remained the condition with the highest total success rate and lowest login time.

As shown on Table 5.7, there were some participants on each condition who they needed to have more attempts in order to successfully recall their passphrases and login. This number ranged between 5 to 19% across all conditions, with CC having the lowest and Repetition the highest rate.

		Success first attempt	More attempts	Avg login	Total success
Conditions	CC-SP	83.54%	5.06%	13.74	88.61%
	Control	51.39%	5.56%	45.78	56.94%
	CC	76.81%	4.35%	22.08	81.16%
	SP	68.57%	8.57%	25.67	77.14%
	Repetition	57.14%	19.94%	49.89	65.08%
	Recognition	51.95%	7.79%	30.45	59.74%
	CC-SP w/o Cue	60.00%	5.71%	37.87	65.71%

Table 5.7 Third login session total success rate percentages, the percentages of those who needed more attempts to login, and average login duration (in seconds) for each condition.

5.4.5 Login Time

We hypothesized there will be a significant improvement in time required to login. The null hypothesis assumes the distribution of login time for the conditions are equal. p values less then .05 will reject this hypothesis and approves the alternative hypothesis. Running the MWU test, for the third login session, there was a significant difference for the login time of the CC-SP condition compared to the Control condition ($p < .001$). The comparison between SP and CC-SP also showed a significant difference between the login time for the third session ($p < .001$). The pairwise comparison of CC-SP and CC also showed a significant difference in the login time ($p < .001$). We also evaluated if there is any significant difference between CC and Repetition as well as SP and Recognition. Our analysis confirmed, the login time for the third session of CC and Repetition and SP and Recognition also had significant differences for the login time ($p < .001$). Since there was no cue for the login session of CC-SP w/o Cue and Control, we evaluated if there is any difference between these two conditions for the third login sessions. Our analysis also confirmed there difference exists and the participants had improved login time given the provided training for their assigned passphrases.

5.4.6 Pairwise Comparisons

As per our main research questions, we want to know if the combination of two implicit memory techniques could improve memorability of system-assigned passphrases. Our findings confirmed the usability benefits of the proposed approach; however, we were also interested in finding out which IL technique is the most effective; that is, CC, SP, or the combination of both. To answer this question, we designed two other experimental conditions, one for CC and one for SP solely. Pairwise comparison of CC-SP and CC conditions total authentication success rate for the third login session did not show significant difference of performance between the two conditions with $\chi^2 = 1.06$, $p = .3$. It is interesting to note, although there was no significant difference for the login success rate, the average login time has a statistically significant difference between CC-SP and CC ($p < .001$). Pairwise comparison of CC-SP and SP conditions authentication success rate for the third login session did not show statistical significant difference $\chi^2 = 4.63$, $p = .03$ ($HC\alpha = .01$). Figure 5.5 shows how different conditions had statistically significant success rates on the login success rate for the third login session.

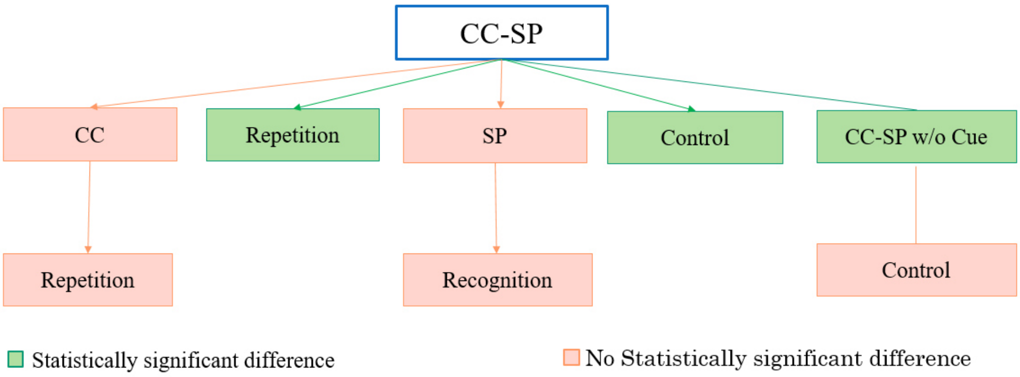

CC-SP
CC
Repetition
SP
Control
CC-SP w/o Cue
Repetition
Recognition
Control
🟩 Statistically significant difference
🟥 No Statistically significant difference

Fig. 5.5 Pairwise comparison of the experimental conditions for authentication success rate for the third login session. The green rectangles show significant difference whereas the orange ones indicate no statistically significant difference.

Conditions	*p-value*	HC
CC-SP and Control	$< .001$	0.006
CC-SP and CC	0.3	0.012
CC-SP and SP	0.03	0.01
CC-SP and Repetition	0.004	0.008
CC-SP and CC-SP w/o Cue	0.001	0.007
CC and Repetition	0.03	0.01
SP and Recognition	0.5	0.012
Control and CC-SP w/o Cue	0.3	0.012

Table 5.8 The results of Chi-Square for the pairwise comparison for the success rate for the experimental conditions. Holm-Bonferroni Correction (HC) was applied on the set of 8 pairwise tests for the S3 success rates. HC column shows the updated alpha value for achieving significance. The highlighted rows show the conditions with statistical significant difference.

We also included a Repetition condition to examine if the usability improvements of our approach are due to repetitions in the training phase and recognition in the login phase. Pairwise comparison of CC and Repetition condition's total authentication success rate for the third login session did not show significant differences, $\chi^2 = 5.07$, $p = .03$ ($HC\alpha = .01$). It is worth noting that CC alone might be significantly better than Repetition, as it was significant prior to correction (and was quite close even after).

The same analysis was performed to evaluate if the effectiveness of our IL-based approach is due to SP, or the participants just recognize the words without any help from the semantic relation of the words. To evaluate this, we performed a pairwise comparison of the success rates for the third session of the SP and the Recognition conditions, finding that there is no significant difference in performance with between the two conditions $\chi^2 = .38$, $p = .5$.

We hypothesized the provided training is effective enough to help users recall their assigned passphrase without providing cues in the login session. By including CC-SP w/o Cue condition, we aimed to find out if the effectiveness of the CC-SP training can still exist even without providing cues for the login session. The recall success rate for this condition was not as promising as the CC-SP condition. Pairwise comparison of this condition with

CC-SP showed a significant difference for the third login session success rate (χ^2 = 11.28, p = .001). This rejects the hypothesis that removing cues does not affect the effectiveness of the approach. In order to compare this condition with the Control condition we performed a pairwise comparison of the CC-SP w/o Cue and Control condition's total authentication success rate for the third login session showed no significant differences between the two conditions (χ^2 = 1.06, p = .3).

We also performed pairwise comparison for the required login time to find if there is any statistical significant difference between different pairs. Our analysis confirmed the login time could be affected depending on the training and the provided cue. Figure 5.6 indicates if there was any difference.

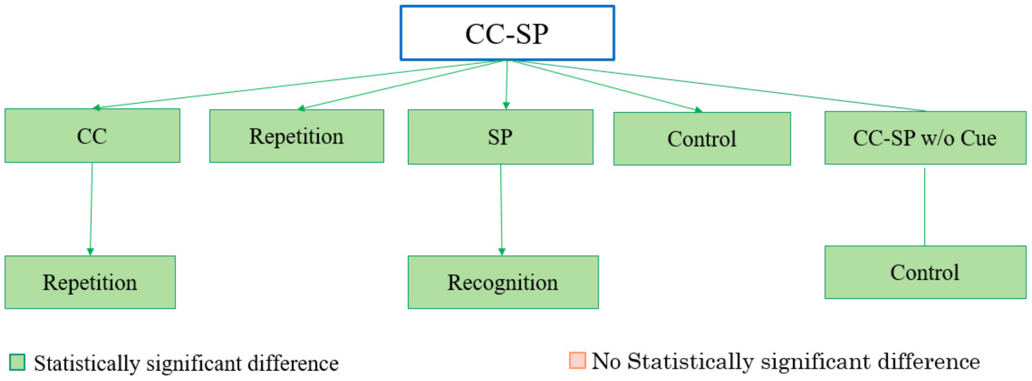

CC-SP
CC
Repetition
SP
Control
CC-SP w/o Cue
Repetition
Recognition
Control
🟩 Statistically significant difference
🟧 No Statistically significant difference

Fig. 5.6 Pairwise comparison of the experimental conditions for the login time of the third login session. The green rectangles show significant difference whereas the orange ones indicate no statistically significant difference.

5.5 Users Sentiments

As per $H_{usability-susscore}$, we hypothesized there will be a significant improvement in user sentiment in IL-based trained passphrases compared to the control conditions. A variety of questionnaires have been used for assessing the perceived usability of interactive systems. To

Conditions	*p-value*	HC
CC-SP and Control	$< .001$	0.006
CC-SP and CC	$< .001$	0.006
CC-SP and SP	$< .001$	0.006
CC-SP and Repetition	$< .001$	0.006
CC-SP and CC-SP w/o Cue	$< .001$	0.006
CC and Repetition	$< .001$	0.006
SP and Recognition	$< .001$	0.006
Control and CC-SP w/o Cue	$< .001$	0.006

Table 5.9 The results of MWU test for the pairwise comparison for the login time for the experimental conditions. Holm-Bonferroni Correction (HC) was applied on the set of 8 pairwise tests for the S3 login times. HC column shows the updated alpha value for achieving significance. The highlighted rows show the conditions with statistical significant difference.

assess subjective reactions that participants in a usability test had to our system, we used the SUS (System Usability Scale) [134]. We also included some other questions to evaluate users' sentiment about the scheme. Figure 5.7 and 5.8 show an overview of the responses of the participants in the CC-SP and Control conditions. For CC-SP condition participants most of the participants did not find the system boring, or difficult to use compared to passwords. We also asked them: *"Given that the training session teaches you a system-assigned passphrase, which provides more security, would you use it instead of a regular password?"*, for different types of accounts. The majority of the participants showed interest in using our approach for online-banking or email accounts.

We also included the responses of the participants in CC-SP w/o Cue group to evaluate how removing the cues for login would affect users' experience recalling their assigned passphrase given our provided training. Figure 5.9 indicates an overview of the responses to our post experimental questionnaire.

To evaluate the result of the SUS questions, we converted the participants score for each question to a number based on the question. Table 5.10 shows the average score for each condition. As shown on this table CC-SP has the highest score which confirms user's

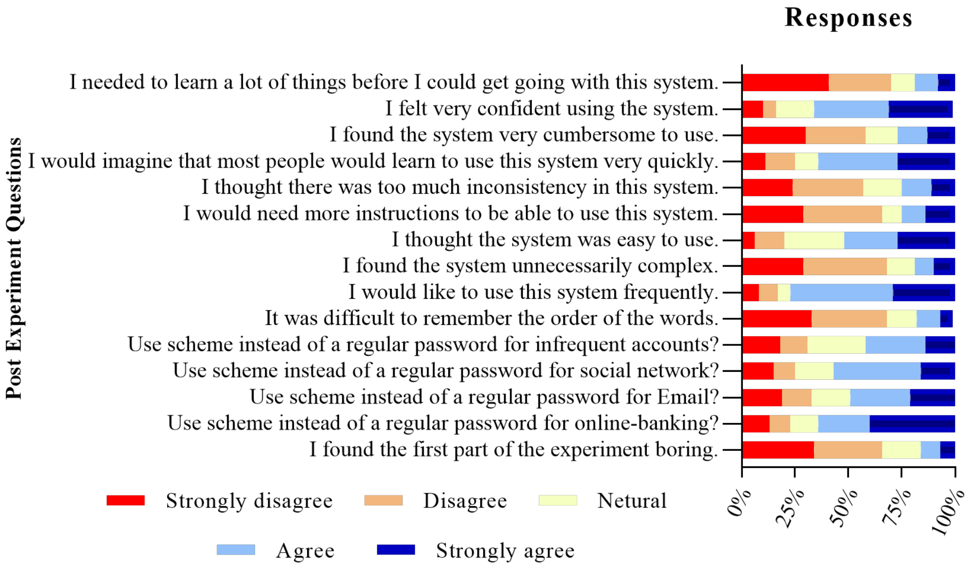


Fig. 5.7 Likert response data on the post experimental questionnaire for the CC-SP condition participants.

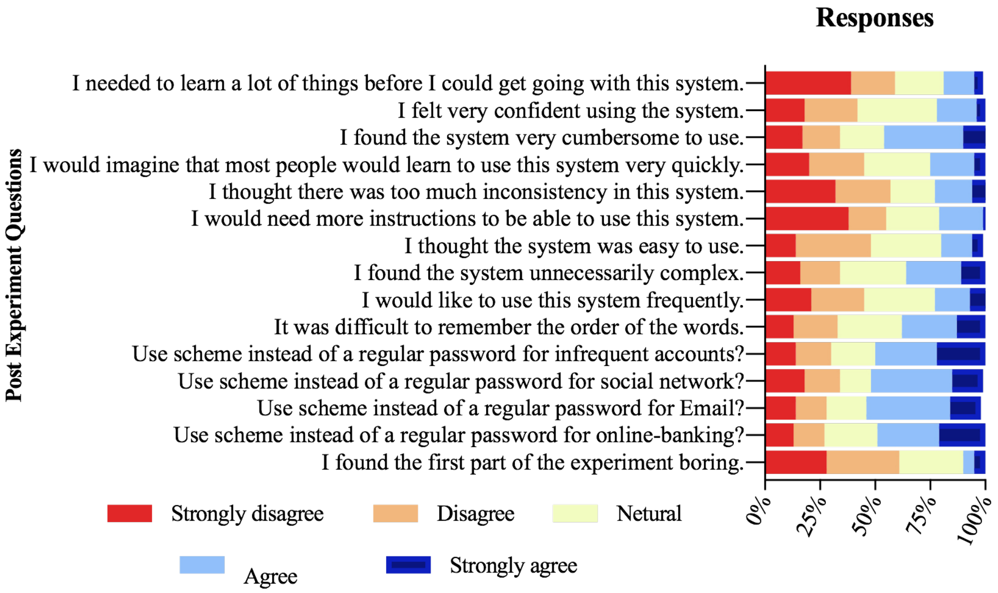


Fig. 5.8 Likert response data on the post experimental questionnaire for the Control condition participants.

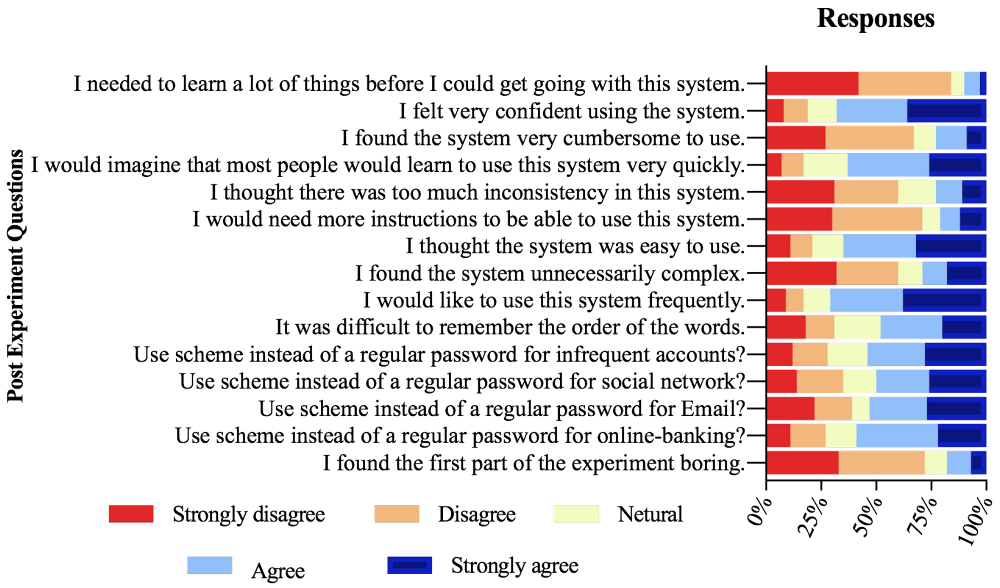


Fig. 5.9 Likert response data on the post experimental questionnaire for the CC-SP w/o Cue condition participants.

positive sentiment regarding the approach. The score for all other conditions is almost the same except for the Control condition. A SUS score above 68 would be considered above average and anything below 68 is below average [135]. As shown on Table 5.10 some of the conditions have received a score over 68 and some under 68. The Control condition has the lowest score of 59.62. Since the participants were not provided with any training and/or no cue for the login, they showed more negative sentiment towards this condition where the participants in CC-SP have shown more positive attitudes towards the approach. This can be an indication that our IL-based interface improved usability. The scores for other conditions have turned out to be almost similar which is interesting and can imply that providing training can improve user sentiment about the system. Another interesting outcome of the table is the difference of the scores for CC-SP and CC-SP w/o Cue. This will confirm that the approach will provide better outcome when the training is complemented with login cues.

Condition	SUS score
CC-SP	75.86
Control	59.62
CC	69.51
SP	67.73
Repetition	64.19
Recognition	67.69
CC-SP w/o Cue	68.10

Table 5.10 The average SUS score for participants of each group.

Since the CC-SP performed better than all conditions, we also evaluated the participants' responses to each question of the post survey in order to find out if there are statistically significant differences between the participants' responses in this group compared to the control condition. Running the MWU test, we found statistically significant differences between the responses for most of the questions. Table 5.11 shows the *p* value for the questions with a statistically significant difference. As shown on the table, participants show more positive sentiment in the CC-SP condition compared to the Control condition.

	Question	*p* value
Conditions	For more security I would like to use it instead of passwords for:	
	online banking	0.000
	email	0.002
	social network	0.004
	It was difficult to remember the order of the words	.000
	I would like to use this system frequently for more secure authentication	0.009
	I thought the system was easy to use	0.001
	I found the system very cumbersome to use	0.01
	I felt very confident using the system	0.000

Table 5.11 The result of MWU test shows statistically significant difference for the responses of the participants in CC-SP condition compared to the Control condition. All results were in favour of CC-SP.

For the question where we asked "It was difficult to remember the order of the words", the Control condition received the highest rank as the participants needed to fill the four words in four text boxes and it was difficult to remember them. Although the CC-SP w/o Cue did not provide any cues for the login session and the participants needed to type the words in text boxes, this score was not as low as the Control condition for the CC-SP w/o Cue condition. This implies that the provided training will provide a better memorization process in the users' mind for the order of the words. For the question "I found the system very cumbersome to use", the Repetition condition received the lowest score as the participants were provided with some random displays which they can not make any relation between the words and it made it difficult for them to recall the words later.

5.6 UDS Framework

We end our discussion with an overview of the usability, deployability, and security properties, using a modified version of the web authentication framework of Bonneau et al. [136]. Our analysis is performed for the CC-SP condition which outperformed other conditions (see Table 5.12).

In terms of usability measures, our approach outperforms passwords in a few ways. Our approach is *Quasi-Physically-Effortless* as users only need to click (or on a touchscreen, touch) on the words after they find the passphrase word. The simplicity of our approach makes it *Easy-to-Learn* as per our questionnaire, 96% of the participants did not find a need for learning a lot of things before using the system and thus did not have difficulties to use the approach. The short length of the login phase means that it is *Efficient-to-Use*. Comparing to the required time to type a system assigned 5-character password (mean 27.5s, two days later [123]), CC-SP is *Efficient-to-Use* (mean 13s 1 week later). Our authentication success rates were very high (88%, one week later), and since the users do not need to type their passphrase, IRPP has *Infrequent Errors* and performs better than system-assigned passphrases (57%, one week later in our Control group; 44% 2 days later [123]). To offer the *Easy-Recovery-from-Loss* benefit, the approach needs to provide convenience when the credentials are lost or forgotten to regain a new authentication secret. The required training time for assigning a new passphrase is 64 seconds on average, making our approach worse than passwords for offering *Easy-Recovery-from-Loss*.

Our approach does not offer the *Accessible* benefit, as users need to be literate in order to read the word displays and understand the semantic relation of the words. Our approach also has *Negligible-Cost-per-User*. It is not *Server-Compatible* as its implementation is quite different than regular passwords; however, it is *Browser-Compatible* as users do not have to change their client to support the scheme. It is clear that our approach is not *Mature*. Anyone can implement or use this approach; thus, it is *Non-Proprietary*.

It is also *Resilient-to-Theft* as the authentication information is in the user's memory. Since our approach assigns random passphrases to users, we rate it as *Resilient-to-Targeted-Impersonation* and *Resilient-to-Leaks-from-Other-Verifiers*. Our approach is also *Unlinkable* since each system should assign a passphrase randomly; we rate this as better than passwords, as in cases where a user reuses their password, their accounts could be linked with some probability.

IRPP is also *Resilient-to-Phishing*, considering classical phishing attacks, wherein the attacker creates a phishing site that mimics the IRPP login process. Through this attack, the attacker attempts to trick the user into responding to the provided challenges and thus find the passphrase words. In CC, the four displays that users are challenged with contain random words. We first enumerate the number of possible displays that can be generated based on our system design for CC and we denote this set with $|D|$. Since we use a dictionary of 923 words to select the words from, and each display is a 6×11 matrix containing 32 words, then for the first display the possible number of displays to challenge users with would be $|D_1| = {}_{923}C_{32} \times {}_{66}C_1 \times {}_{65}C_{31} = 2^{264}$. Since the words are unique for each display, then $|D_2| = {}_{891}C_{32} \times {}_{66}C_1 \times {}_{65}C_{31}$, and $|D_3| = {}_{859}C_{32} \times {}_{66}C_1 \times {}_{65}C_{31}$, $|D_4| = {}_{827}C_{32} \times {}_{66}C_1 \times {}_{65}C_{31}$ for the third and fourth displays accordingly. This scenario assumes that the users learn the locations of all the words and once the locations are changed they notice this display is not part of their assigned passphrase. For the first display, since there are 2^{264} possible displays to challenge the user with, and each login session should only contain 4 displays, we expect it would take over $2^{264}/4 = 2^{262}$ phishing attempts on the same target user i to successfully recover i's passphrase and the same would be applied for the rest of displays. However, as we have not tested such a scenario, we don't know what cues users can detect as to whether the displays are different than what is normally presented to them at login time. The worst case scenario would be if the location of the target word on the display does not matter, in the sense that the user cannot detect such differences. For this worst case scenario, the attacker could create 923/32 =28 unique sets of words that appear on a display, where the words are placed in any locations. Then there are $28 \times 27 \times 26 \times 25 = 2^{19}$ ways to show the sequence of displays. For SP, we made displays containing words with semantic relations. We formed a set of 40 word displays with their corresponding semantically related words. For a phishing attack, we assume the attacker knows the 40 sets of words we used. As per the current configuration of our system, the possible number of sequences of four displays that can be generated for SP would be $|D| = 40 \times 39 \times 38 \times 37 = 2^{21}$. Since there are 2^{21} possible display sequences to challenge the user with, we expect it would take over 2^{20} phishing attempts on the same target user i to successfully recover i's passphrase. It should be mentioned that that user would recognize that the display's distractor words are not semantically related to each other (otherwise, the attacker could do the same attack as for CC using 28 displays containing unrelated words). It is also worth noting that the dataset that we used has a potential to be further improved in order to provide more semantically related words, and thus be able to produce more displays.

For CC-SP, we have both CC and SP. With SP we have the semantic relation of the words to be considered on each display, and CC to place these words on 66 possible locations of each display. Given the set of 40 possible SP word groupings that we ran our experiment with, the attacker first needs to guess the word, and then the location to recreate each display. For each display, the position of the target word is chosen: ${}_{66}C_1$. Then the position of each of the 31 prime words is chosen: ${}_{65}C_{31}$ which results in $66 \times {}_{65}C_{31} = 2^{67}$. the possible number of sequences of four displays that can be generated for SP would be $|D| = 40 \times 39 \times 38 \times 37 = 2^{21}$. Since there are 2^{21} possible display sequences with possible 2^{67} possible configurations of the display ($2^{67} \times 2^{21} = 2^{98}$) to challenge the user with, we expect it would take over 2^{97} phishing attempts on the same target user i to successfully recover i's passphrase.

Our approach has *No-Trusted-Third-Party*. It also offers the benefit of *Requiring-Explicit-Consent* since the authentication relies on a conscious consented user.

Table 5.12 Comparing our approach vs. passwords and system-assigned passphrases using the UDS framework [3]. Our approach performs better than passwords and system-assigned passphrases in terms of usability and security.

	Memorywise-Effortless	Scalable-for-Users	Nothing-to-Carry	Physically-Effortless	Easy-to-Learn	Efficient-to-Use	Infrequent-Errors	Easy-Recovery-from-Loss	Accessible	Negligible-Cost-per-User	Server-Compatible	Browser-Compatible	Mature	Non-Proprietary	Res.-to-Physical-Observation	Res.-to-Targeted-Impersonation	Res.-to-Throttled-Guessing	Res.-to-Unthrottled-Guessing	Res.-to-Internal-Observation	Res.-to-Leaks-from-Other-Verifiers	Res.-to-Phishing	Res.-to-Theft	No-Trusted-Third-Party	Requiring-Explicit-Consent	Unlinkable
Web Passwords			●		●	●	○	●	●	●	●	●	●	●		○						●	●	●	●
System-Assigned Passphrase	≡		●		○	○	≡	●	≡	●	●	●	≡	●		●|||	●|||	●|||		●|||		●	●	●	●|||
CC-SP Passphrase	○|||		●	○|||	●	●	●|||	○	≡	●	≡	●	≡	●		●|||	●|||			●|||	●|||	●	●	●	●|||
CC-SP w/o Cue Passphrase	○|||		●		●	●	≡	○	≡	●	≡	●	≡	●		●|||	●|||	●|||		●|||		●	●	●	●|||

● – offers the benefit, ○ – almost offers the benefit, no icon – does not offer the benefit, ||| – better than passwords, ≡ – worse than passwords

5.7 Discussion

I proposed an approach enabled by implicit learning in order to facilitate memorability of system-assigned authentication secrets. Through an online study, I evaluated different conditions and found the IL-based training could improve memorability of system-assigned passphrases. I studied the memorability of system-assigned passphrases through a large-scale online user study, focusing on the effects implicit learning for memorization and retrieval of passphrases. The results suggest that when the two implicit learning techniques, CC and SP, are combined and used to train users on system-assigned passphrases, we can have the best short- term and long-term memorability. In this section, I discuss the results and summarize the high-level findings.

To evaluate effectiveness of employing implicit learning for memorization of authentication tokens, we designed, implemented, and tested an approach enabled by implicit learning. We were aiming to find if we can gain any memorability improvements through our proposed approach. To train users on a system assigned passphrase, we assigned them seven different experimental conditions. Each condition contained a single or combination of some factors in order to find whether the incorporated factors are effective when they are used solely, or they are effective when combined.

We started our analysis by the pairwise comparison of CC-SP versus Control. CC-SP included the two CC and SP effects while Control did not provide any training for the users. This comparison allowed us to evaluate effectiveness of our proposed implicit learning-based approach for memorability of system-assigned authentication tokens. Our analysis confirmed statistical significant differences for authentication success rate, login time, and storage behaviour between these two experimental conditions, confirming the effectiveness of such a training for memorability of system-assigned passphrases. This implicit learning enabled training, facilitated user's memorization process and helping them to recall their assigned passphrase more efficiently. This condition outperforms all other conditions, confirming that memory encoding is more effective when a set of semantically related words are presented repeatedly in a limited time on preserved locations. While our special training turned out to be the most effective condition in terms of memorability, storage behaviour, and users acceptance, included CC and SP, we were needed to tease out how the effectiveness of different factors would be in this process.

Including two other conditions; i.e., CC and SP, allowed us to find if these two methods can provide significant memorability benefits when they are employed solely. This will also help us to have a sound evaluation to find if the effectiveness of CC-SP is due to SP, CC, or both.

Our results did not show significant memorability advantages for SP compared to CC-SP when it was used alone; however, CC still provided significant memorability benefits compared to SP, although the provided memorability improvement was not as effective as CC-SP. It is worth noting that before applying Holm-Bonferroni corrections, we found statistically significant difference for the authentication success rate of CC-SP compared to SP, confirming CC-SP being more effective than SP alone; however, applying the corrections made the difference insignificant which could still be considered as nearly significant. This suggests that SP also provides memorability benefits; however, due to the fact that the difference between CC-SP and SP is nearly significant, we can state that CC is a more important factor for memorization improvement of CC-SP compared to SP. While the comparison of CC-SP and SP did not show a significant difference, the comparison of CC-SP and CC did not show any significant statistical differences confirming the effectiveness of CC when it is used solely. This is an indicator of CC being more effective for the memorization process than SP.

The Repetition condition was included into the study as a control condition for CC-SP to find out if the repeated exposure of a set of unrelated items can improve memorability. The pairwise comparison of CC-SP and Repetition confirmed a statistical significant difference between the two conditions asserting that CC-SP with the special training involved can have effective memorization process through which users are able to be triggered in an effective way by what they learnt during the training phase and cues during login that eventually helped them to recall their passphrase.

Since CC includes different factors such as repetition, preserved location, and exposure time, we included a control condition for CC, Repetition, to find if repeated exposure of a set of words for the same time duration can provide memorability benefits. For this pairwise comparison, before applying the HC corrections, our results showed statistically significant differences for the authentication success rates of these two conditions. Meaning that repeated exposure of the words cannot provide memorability improvements and for this type of cue to be as effective as CC; it needs to be complemented by preserved location of the words. However, after applying the HC corrections, the difference between the two conditions turned out to be insignificant or better to be said nearly significant as the difference between the p-value and HC corrected alpha is small. Interpreting the results with the HC corrections, suggests that repeated exposure of a set of unrelated items can facilitate memorization of them.

Including Recognition in the experiments allowed us to find out if providing some unrelated words for the training and login can result in better memorability. Comparison of this condition with SP, did not show any significant improvement for memorability; however, resulted in decreasing login time. This shows that, although there is no improvement in the authentication success rate, it can improve login time as a result of more effective training.

Another interesting take away based on the results was the fact that login cues will improve users' retrieval process. Including CC-SP without cues, showed a drop in the performance of the approach, indicating the importance of the cues for the login. A statistical significant difference in the authentication success rates of CC-SP versus CC-SP w/o Cues confirmed that for users to make better mental encoding of their assigned passphrase, rather than the provided training session with proper mechanisms, they need to have the cues for the login for better retrieve the stored information; however, it is possible with more training or login sessions, users do not need the cues and can rely on their memory without any cue.

It is noteworthy that CC-SP w/o cue did not show significant difference for the success rate compared to Control. This interesting result validates our special training needs the cues in order to have more effective retrieval.

5.7.1 Storing Behaviour

Interestingly, the tendency for storing passphrases received the lowest percentage (7%) for CC-SP and CC-SP w/o Cue. This can be an indication for these two conditions to have sufficient training that users were confident enough to not store their system-assigned secrets. Although CC-SP w/o Cue did not perform well compared to CC-SP, participants found the scheme effective at the training time, so did not store the secrets. However, they failed for the login session as cues were needed for a successful memory aid. Storing rates for the Repetition and Recognition conditions had the second highest score, this suggests that the participants were not finding as much pattern or memory cues to facilitate memorization of the words. For these two conditions, as there was neither consistent locations of the words (as in CC) nor semantic relation between the words (SP), this rate was much higher compared to other conditions, such as CC and SP which had some kinds of implicit memory training.

5.7.2 Common Errors

As we had two conditions therein users needed to input their passphrase (as opposed to the other conditions that they needed to click on passphrase words), a deeper analysis of the data, showed the common errors for CC-SP w/o Cue were swapping the words which indicates participants had problems with the order of words. Providing cues can prevent such errors. This issue was not a common mistake for the Control condition though. Of those in CC-SP w/o Cue who swapped the words 9% had recalled all four words; however, in wrong order. This number was 1% for the Control condition. If we consider different ordering of the correct words as a correct input, authentication success rate for CC-SP w/o Cue third login session rises to 75%. Such a consideration can substantially improve login success rate for CC-SP w/o Cue compared to the Control condition which results in a statistical significant difference of authentication success rate with $\chi^2 = 5.58, p = .01$). This difference is significant only prior to HC correction (HC alpha =0.007). However, the low p-value suggests that this may be significant and is worth further study in the future. As we had a spell checker on each text box, we did not find any typos or other mistakes that can be fixed with some corrections. Thus, their inputs were either completely off, or having the a common mistake of swapping words. Of interest is those in CC-SP w/o Cue who could recall parts of their passphrase, but not all of the words (one word 14%, two words 11%, and three words 7%). These numbers are the percentages of users who recalled exactly the reported number of words. For the Control condition we found these results as: (one word 10%, two words 7%, and three words 2%).

5.7.3 Fading Effects

We define "fading effect' as the rate of forgetting memorized authentication secrets over the course of time. In order to find out how the fading effect of memorized passphrase is for each condition, we plot the success rates related to all three sessions for all seven conditions. Figure 5.10 shows how the success rate decreases over time. As shown on this table, Recognition and Control have the most dramatic decrease for this effect. As the participants in the Control condition were provided with system-assigned passphrases and no training or login was provided for them, the fading effect makes sense; however, among other conditions which users had training and also were provided with cues, Recognition condition had the highest rate of fading. This suggests semantically related words (i.e., SP) for the training can slow down the fading effect. The fading effect for the CC-SP w/o Cue and Repetition conditions have almost the same rates.

Based on our analysis, the login time also increases over time, most likely because of memory decay; however, this rate is much lower for CC-SP compared to the other conditions. As shown in Figure 5.10, fading of the memory for the Control, Recognition, and Repetition

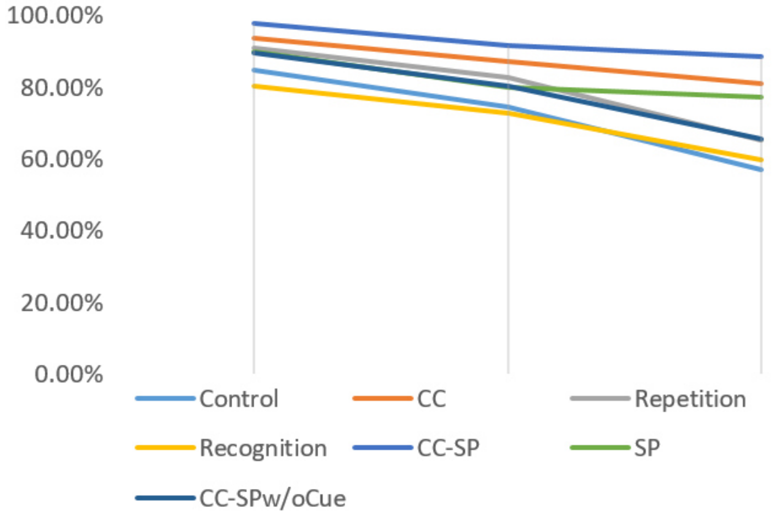


Fig. 5.10 Fading effect of memorized passphrases across all conditions.

conditions wherein no implicit memory training was provided, happens much faster than other conditions. This confirms the effectiveness of the two employed implicit learning paradigms. However, for CC-SP w/o Cue that had training equipped with CC and SP, the fading rate is almost identical to the Control condition. This is an indication of the requirement for the cues to trigger implicit memory of users. Removing cues completely as done in this test has negative a effect on memorability.

5.7.4 SUS Scores

Users' perception of any new approach has a direct impact on how they accept it. As per the user sentiment analysis, those participants who had better performance on the task had more positive sentiment towards the approach. The SUS score evaluation also resulted in CC-SP with the highest score and Control with the lowest. For the Control condition participants with no training and login cues, the sentiment was more negative, likely due to multiple failures. Although the recall rate for the CC-SP w/o Cue condition was not as promising as CC-SP, participants' sentiment was less negative. Users' sentiment is also in a direct relation to the login time. The negative sentiment users have towards the system can be due to different reasons such as longer login time (after multiple failures) or memory frustration. For the third login session, among all conditions, participants in Repetition had the highest rate to need more attempts for successful login and as a result a longer login time. This can be due to the fact that if there is no pattern to be caught by users, repetition may not be effective and it can only cause more cognitive load and distraction. As shown in Table 5.10 Repetition got the second lowest SUS score among all conditions which again confirms how this method of training can have negative effects. For CC and SP, although some memory cues were provided for the training and login, they were not as effective as when the two are combined. The combination of these two implicit learning techniques enhanced the performance and thus affected users' sentiment.

All aforementioned discussion of the results suggests a conclusion that if memory is triggered in an effective way, it can improve memorability of system-assigned authentication secrets. However, for the two paradigms that we used, they are most effective when cues are provided for the login. However, it is possible after a few login sessions, users do not need to have cues and authentication secrets can be recalled even without cue. This needs a long term future study to find if after a number of login sessions, without providing cues, users are able to recall their assigned passphrases. It would also be interesting to study after the first training session, if users do not try any login session, for how long the knowledge is still accessible from their implicit memory.

5.7.5 Summary of Results

Given the promising results of Tacit Secrets, I was aiming to take advantage of implicit memory techniques indirectly in order to reinforce memorability of system assigned passphrases. Providing a training mechanism enabled by implicit learning, I designed an approach, called "Implicitly Reinforced Passphrases". The proposed approach, employs users' implicit memory to train them on a 4-word system-assigned passphrase. The training mechanism facilitated the memorization process and thus recalling later. To evaluate the feasibility of the approach, I ran an 880-participant online study and explored usability of the approach compared to a set of control conditions.

The feasibility study showed that the proposed approach improves usability of system-assigned passphrases, both in terms of recall rates and login time. 88.61% of the participants who were trained through the special IL-based interface, were able to recall their passphrase successfully seven days after the training. Besides the effectiveness of the provided training, since there is no need for users to type their assigned passphrase words, it can prevent increased typographic errors which is a common drawback for passphrases [63]. Preventing such errors can prevent login failures; therefore, can positively affect users' perceptions of the approach.

The participants recording behaviour was also different across the conditions. Our analysis confirmed existence of a significant difference in recording behaviour of the CC-SP condition compared to the Control condition ($\chi^2 = 29.61, p < .001$) confirming the effectiveness of training. Performing pairwise comparsions for the login time of different conditions, we found significant differences in these conditions. While CC-SP had the shortest login time, participants in the Control condition needed more time to login. This was due to the fact that they first needed to recall and then type the words. Since they had difficulties to remember their assigned passphrases, they needed more login attempts.

5.8 Limitations

While we strove to provide users with a scenario which ask them for the importance of such authentication scheme, we could not do so perfectly. Users usually care more about their actual accounts in the real world. The more actual and sensitive the account is, the more endeavor they make.

Participants may have wanted to please the researchers by giving a more positive answer to our sentiment question, which asked whether they they are willing to use the scheme for different online accounts.

While the participant were required to perform the task on a desktop device, we assumed they are using mouse to click on the words; however, we did not log what type of screen they are interacting with. While it is possible that using different input device could impact users' login time, it would interesting to verify what type of display they used (e.g., touch display vs mouse).

As per our study related to Tacit Secrets, we found how including eye-tracking device can improve performance of the approach. For Implicitly Reinforced Passphrases, we were aiming to evaluate our proposed approach performance in a large scale, using Mechanical Turk. Using Mechanical Turk allowed us to collect data for large number of participants; however, we were not able to include eye-tracking data as the users were performing the task in their own location with no eye tracking device. It would be an interesting venue for the future work to evaluate performance of Implicitly Reinforced Passphrases when the study is equipped with eye-tracking device and find out its effect on the results.

5.9 Ecological Validity

For this authentication approach, there are different factors that may affect the ecological validity of the study. Passphrases are not as well-known as passwords to the users, such unfamiliarity can possibly affect the way they interact with the system. The more experience they gain, the more natural behaviours they have. Another ecological validity issue related to authentication studies is that participants do not put as much efforts as that of they put for their valued sensitive accounts. This may result in less effort to memorize or recall their assigned passphrase.

The participants performed the study through an online system where they were involved in their usual physical environments, without the intervention of any experimental equipment or person. While this may be better than a lab environment in some ways, using MTurk means that our participants may have been less motivated and/or more rushed than usual. Regardless of any issues associated with the use of MTurk, our comparison to control groups should still provide useful evidence of whether our approach yields an improvement.

5.10 Conclusion and Future Directions

Our indirect implicit learning-based authentication secrets results indicate that implicit learning techniques can be used to reinforce memory for system-assigned passphrases. Our proposed approach aims at overcoming an effortful authentication experience for system-assigned secrets. Hun et al. [137] found 6-digit system-assigned PINs to have a 56% success rate 2 days after training. The usability of CC-SP is much better than these systems as it has high memorability (88% success rate one week later) and infrequent login errors.

CC-SP also is much better than these systems as it has faster login times (mean 13s 1 week later) which is much faster than system-assigned 6-digit PINs (mean 41.7s [137]) and system-assigned 5-char passwords (mean 27.5s [123]) 2 days later.

It is worth noting however that user-chosen PINs or passwords have shorter login times, but these are not comparable in terms of security.

CC-SP also involves a relatively short one time training cost (at most 100 seconds, with a mean time of 64 seconds). Since forgetting passwords can have consequences in terms of money (e.g., IT helpdesk costs) and time, and can take up to two hours before it has propagated to all the systems [138, 139], one can view this approx. 1 minute training as worthwhile given the reduced number of forgotten passphrases, which reduces the number of resets.

Thus, the proposed approach offers an improved balance of usability and security as previous approaches to system-assigned PINs [137] and passwords [123] with comparable security have longer login time, poor memorability, and thus frequent input errors. User-chosen passwords are no longer resistant to online guessing attacks, as demonstrated by Wang et al. [10] guessing 32-73% of passwords within 100 attempts. CC-SP also has the added benefit of phishing resistance and according to Thomas et al. [140], phishing and leaks from other verifiers are currently two important threats that lead to credential theft.

In future work, to improve security of Implicitly Reinforced Passphrases against offline attacks, for one of the experimental conditions, CC-SP w/o Cues, we removed cues for the login session. Although there was insignificant improvement, the recall rate for the participants in this group was not as high as those of CC-SP who were provided with cues for the login session. Thus, we found the cues are required for significantly improved recall. One future direction can be to improve resilience to phishing, even against targeted phishing attacks, by using a technique used by Cued Click-Points (CCP) proposed by Chiasson et al. [141]. To improve security, CCP uses one click-point on each image (from a sequence of five images). The next image is displayed based on the location of the previously chosen click-point. Implicitly Reinforced Passphrases can be considered in a same way wherein images are word displays and click-points are the word of the passphrase. Users are exposed to four displays and need to select words of their passphrase from therein. Depending on what word they click on each display, the next display can be changed. Choosing the right word of the passphrase results in the next display to be the display related to the next passphrase word, whereas the wrong selection winds up in exposing an unrelated random display. Such an amendment could improve security of the scheme when an attacker tries to harvest displays for a targeted phishing attack, they will wind up with an incorrect sequence of displays to present the user with.

There is another venue for future work to find out if increasing the number of displays and/or distractors on each display; e.g., having 6 displays instead of 4, or 5 displays with twice as many distractors would result increased keyspace and thus security of the approach. Another interesting future work is to evaluate if there is any correlations between assigned passphrases and users' memory strength characteristics.

Chapter 6

Discussion

In several psychological studies of human memory, it has been suggested that the phenomenon of "forgetting" is essentially a retrieval problem. The information could be stored in the memory, but we are not able to find the right way to retrieve it. In order to facilitate memorization and retrieval, we use memory aids. Human memory retrieval process is triggered by retrieval of cues. These cues can be some stimuli related to a previous experience that facilitate the recall of other information related to the same experience. This is what we used by incorporating CC effect. We manipulated implicit memory in order to improve recall. Examples of effective cues for retrieval of information can be related to events, time, people, and activities (what and where).

Interest in human memory spans many areas. It has been widely studied in the fields of psychology, philosophy, social sciences, physiology, and of course, computer science, engineering, among many others. In regards to computer science, one of the areas studying users' memory is researches related to authentications. Since the most common authentication scheme, text-based passwords, is solely relying on memory, researchers have long studied several alternatives for text-based passwords. These works were aiming to address different flaws related to this popular authentication scheme. Most of the previous works were focusing "something you know" and users' explicit memory for memorization and recalling authentication secrets. However, using implicit memory can provide several advantages.

In this work, I proposed two authentication approaches enabled by implicit learning in order to improve memorability of system-assigned authentication secrets. In this chapter, I provide a high level discussion of the techniques and results related to the two proposed approaches.

Priming Technique. Over many years of research, numerous proposals on cognitive psychology have studied how different primes can trigger memory. Repetition priming that employs implicit memory, is one of the techniques wherein participants first encode some material into memory and they are later asked to retrieve encoded materials. The more effective the priming is, the more successful retrieval of the encoded materials will be. The interesting aspect related to priming is that it is governed by principles that are different from those of explicit memories. For instance memory impairments that are emerged through aging, brain injury, and disease have different effects on implicit memory compared to explicit memory. So it makes this technique interesting to take advantage of for authentication purposes. As this technique requires some amount of time for encoding data, when used for authentication, it might be criticized for usability flaw. However, considering difficulties to reset a forgotten password, it makes sense to have a a relatively short one-time training cost (at most 90 seconds, with a mean time of 75 seconds for Tacit Secrets and at most 100 seconds, with a mean time of 64 seconds for Implicitly Reinforced Passphrases). Since forgetting passwords can have consequences in terms of money (e.g., IT helpdesk costs) and time which it takes up to two hours before it has propagated to all the systems [138], one can view this ~one minute training as worthwhile given the reduced number of forgotten passphrases, which reduces the number of resets.

Reinforcement Learning. Cognitive psychology considers Reinforcement Learning (RL) as a mechanism that provides the ability to solve sequential decision-making problems with limited feedback. A successful RL mechanism needs a sufficient amount of experience prior to acquiring acceptable behaviour. Acquiring such experience, however, can be costly in terms of data and time [142]. In this chapter, we discuss different aspects related to the two proposed approaches enabled by implicit memory directly and indirectly; that is, Tacit Secrets and Implicitly Reinforced Passphrases accordingly. We discuss more about different performance metrics related to each approach.

6.1 Tacit Secrets

To tackle the problem of insecure user-chosen passwords, different proposals have been suggested by each group researchers in order to force or encourage users to choose secure passwords. For instance passwords meters [143, 144], system-assigned passwords [123], password generators [145], or passphrases [79] are examples of how to improve security of passwords. However, one issue is how to memorize a multitude of secure passwords. To address memorability issues related to these secure authentication secrets, various proposals were introduced. Among the proposed solutions, only password managers can provide a practical solution to retain and retrieve numerous accounts with secure passwords; however, there are various issues such as accessibility, recoverability, and availability [146].

Security experts are usually hesitant of users memorizing strong authentication secrets. This is due to the limitations related to human memory. Different techniques in order to improve memorability of secure authentication secrets. For instance, Bonneau et al. [65] challenged this issue by using the spaced repetition technique in order to facilitate memorability of system-assigned secrets through multiple training sessions. Tacit Secrets uses implicit learning directly through a task in order to train users on a set of displays to be user's system-assigned authentication secret through a single training session. We believe Tacit Secrets is a system-assigned authentication enabled by implicit memory that puts minimum cognitive load on users. However, it needs future work in deepening the understanding of the cognitive and neural underpinnings involved in employing implicit learning for Tacit Secrets in order to find out if the acquired knowledge would be always accessible through implicit memory not explicit memory.

Tacit Secrets Performance Metrics. Providing a training session enabled by CC, we hypothesized users have different distribution of the performance metric (RT, fixation count, or saccade count) for the learnt displays compared to novel displays. The null hypothesis assumed the distribution of performance metrics are equal for both learnt and novel displays. Running the MWU test, the results rejected the null hypothesis and approved RT, fixation count, and saccade counts have different distribution for different types of displays. This allowed us to evaluate users' knowledge with different stimuli and depending on the users' performance, authenticate them. The implicitly acquired knowledge was accessible after a training session which is comparably longer than traditional authentication schemes.

Training Duration. To maintain usability it is desirable to have shorter training session. Following the specifications of the previous CC studies, in our designed approach, we had a training session containing 15 blocks (repetitions). Although it has been shown that implicitly acquired knowledge is accessible after the forth repetition, shortening the training time can come at cost of decreasing durability of the acquired knowledge. If the training session is shortened to make the approach more applicable for variant use cases, we can refresh user's knowledge during each login session. Instead of a training session with 15 blocks, we can have less number of blocks and instead stabilize the knowledge each time user logins by showing some of user's displays. While shortening the training session can improve usability of the approach, increasing the number of displays to be learnt can arguably improve security. As per the current configuration of the approach, each user is assigned a set of 12 displays as their key. Increasing the number of displays to be learnt, linger the training time which comes at cost of compromising the usability. Such an amendment can be made depending on the environment that Tacit Secrets is going to be used for.

Tacit Secrets as an approach that triggers implicit memory can be also used for continuous authentication. Once users are being trained on their assigned secrets, while they are accessing sensitive information, they can be questioned by their secrets.

Tacit Secrets Advantages. A high level comparison of Tacit Secrets with web passwords confirms several memorability and security advantages for Tacit Secrets. That it is *Memorywise-Effortless*, *Scalable-for-Users*, and *Infrequent-Errors* highlight the memorability benefits of the approach. Given the required training time for the approach, due to the memorability benefits it provides, it could be used when seeking more security for different use cases. With regards to security, Tacit Secrets provides several advantages compared to passwords: *Res.-to-Targeted-Impersonation*, *Res.-to-Throttled-Guessing*, *Res.-to-Unthrottled-Guessing*. Kurt et al. [140] recently studied what are the common tools used by attackers in order to perform credential theft. By developing an automated framework they monitored potential theft over the course of March 2016–March 2017. They found 12.4 million accounts were potential victims of phishing attacks. Providing *Res.-to-Phishing*, Tacit Secrets provide an important benefit which traditional passwords do not have it. Being *Res.-to-Coerced-Communication*, Tacit Secrets outperforms most of current authentication approaches for having this benefit.

Implicit Employment of Memory. Tacit Secrets employs implicit learning directly with the goal to mitigate memorability burden and improve recall rates for system-assigned authentication secrets. This is important to confirm if IL is really employed in this approach. Tacit Secrets is purely based on an IL-based task, Contextual Cueing, which is long studied by the cognitive psychology researchers. In order to verify if the knowledge is acquired implicitly, after the completion of the CC task, the participants were provided with a recognition test. They were asked to if they found any similarity/repetition between the displays they saw. Most of the previous studies confirm, participants did not notice any repetition. We followed the design specification of the previous works for the CC task; moreover, through the exit survey of Tacit Secrets task, we also asked our participants if they found any similarity/repetition between the displays. The responses also confirm that the participants were not able to recognize the displays whether they have seen them before or not, which is in line with previous studies.

It is worth noting that we realize that showing a random number of displays in every authentication session may strengthen Tacit Secrets, although determining the security gain of such an approach is left as future work.

In summary, the main advantages of the proposed approach, Tacit Secrets, over system-assigned passwords or PINs are: (1) improved memorability, (2) reduction in input errors, and (3) phishing resistance. Tacit Secrets complicates phishing attacks, as the adversary would need to collect each target user's 4 displays to launch a credible attack. If comparing to a user-chosen passwords or PINs, there are even more advantages. Due to the implicit nature of Tacit Secrets and the authentication measures that are based on the users' implicitly acquired knowledge, Tacit Secrets provide (4) resilience to targeted impersonation. Due to the extraordinary key space of Tacit Secret has (5) resilience to throttled guessing, and (6) unthrottled guessing. Not having user key as clear as text-based password provides more protection for (7) observation attacks than text-based passwords. It also offers (8) resilience to leaks from other verifiers (i.e., password leaks), (9) unlinkability (authentication information from colluding verifiers cannot be used to link the identity), and (10) negligible risk of (throttled) online attacks. It is worth noting that according to Thomas et al. [140], phishing and leaks from other verifiers are currently two important threats that lead to credential theft. The implicit nature of Tacit Secrets make it as one of unique authentication schemes being (11) resilient to key communication in the event of any coercion.

6.2 Implicitly Reinforced Passphrases

Implicitly Reinforced Passphrases as a system-assigned authentication approach, employs implicit learning indirectly through CC and SP paradigms. We examined different hypotheses to find out feasibility of the proposes approach. We hypothesized users in different assigned conditions perform differently depending on the type of training and cues they are provided with for login sessions.

Experiment Conditions. Including different conditions allowed us to find out if there is any improvements in memorability of system-assigned passphrases, what is the key factor for that. So we designed our study to include a set of experimental conditions. For these conditions we performed a set of pairwise comparisons to find if there is significant differences between each condition and its corresponding control condition(s).

Our main goal was to find if our proposed approach enabled by two different implicit learning based paradigms, CC and SP, can improve memorability of system assigned passphrases. This condition, CC-SP, was compared with a set of control conditions. The first and foremost comparison needed to find if this condition provides memorability benefit over the Control condition wherein users are assigned a passphrase with no training and login cues. Our results confirmed the provided training can significantly improve success rate, login time and users' storage behaviour. Users in this condition were more successful in recalling their passphrase in a short time and they have less tendency to store their assign passphrase. This finding was an important take away of this work, confirming the effectiveness of the approach.

While our special training turned out effective in different aspects, we needed to find out how the involved paradigms are improving the memorability. To that end, we included other experimental conditions each as a control to one or more conditions. To find which of the included paradigms is more effective, we included two conditions, one with CC only (non-semantically related words were shown repeatedly in preserved locations), and one with SP (semantically related words were placed on the display with neither repetition nor preserved locations). Our results did not show any significant statistical differences between the these two conditions confirming that they have the same effect on the memorization of the system assigned passphrases.

We continued our analysis by the comparison of CC-SP and CC and SP. For CC, we wanted to confirm if repetition of a set of words can result in effective memory cues, or repetition needs to be completed with preserved locations for the words. Our analysis showed that login success rate dropped when we had repetition of the words, which means users visual spatial system is looking for some cues with more consistency in both the objects and also their locations; however, pairwise comparison of the CC and Repetition conditions did not show significant difference in the authentication success rate while it had a significant difference in the login time. This finding suggests that while CC in used alone or combine with SP in can improve memorability; however, complementing that with SP can expedite the retrieval process as the users in CC-SP were able to recall their passphrase more quickly.

Since we were performing multiple pairwise comparisons, we needed to apply Holm-Bonferroni corrections for the value of alpha. Applying the corrections resulted on some of our pairwise comparisons to no more be significant or be on the borderline (see Table 5.8). If we want to compare the success rate for SP and CC when they are used alone, CC substantially outperforms SP; however, applying the corrections makes SP to have no significant difference with CC-SP. Having a p-value very close to the HC α (i.e., $p = .03, \alpha = .01$) makes us to still consider the difference as being possibly significant and making CC-SP as a more effective training compared to SP. It is also noteworthy that CC-SP had significant differences in the login time with CC-SP having shorter login time.

We then compared Repetition with CC-SP as it was included as a control condition to CC-SP. Our goal was to find if repeated exposure of a set of words can facilitate memorability and recall. Our results indicated a significant difference between the success rates of the users in these two conditions, confirming the effectiveness of the spacial training given the design specifications. This means that any training and/or cue can not necessarily be effective for memorization and recall.

For SP, to verify if the semantic relation of the words matter, we included another condition, Recognition wherein non-semantically related words were exposed to the users.

As expected, the provided cues were not as effective as SP and users' performance were less compared to the SP condition; however, the performance improvement was not statistically significant. While the success rate did not have significant difference, the login time was statistically shorter for the users in SP compared to Recognition. This will confirms the relation of the words can make a better mental encoding and thus recall.

We also compared CC with Repetition to find whether the combination of repetition and recognition can be the source for improved memorability rather than CC. The pairwise comparison of these two conditions was also affected by Holm-Bonferroni corrections. Applying the corrections makes CC to have no significant difference with Repetition. This confirms the effectiveness of Repetition by its own; however, having a p-value on the borderline($p = .03, HC\alpha = .01$) makes us to still consider the difference as being possibly significant and CC alone worth further study. It is also noteworthy that CC had significantly shorter login time than Repetition.

After we found CC-SP outperforms other conditions, we continued our study, by evaluating the CC-SP w/o Cue condition aiming to find if we remove login cues in order to improve security, how users perform. Our results did not turn out as promising as of the CC-SP condition confirming the benefits of the cues for login sessions. However, when we permit swapped word orders in input, the result becomes much better (p=0.01). This p-value would not be significant after HC correction, but it indicates that this approach may be worth further exploration in the future.

Storing Behaviour. To evaluate user's storing behaviour we hypothesized users' will behave differently depending on their assigned experimental conditions. The null hypothesis claimed for dependency between the condition and storing behaviour, assuming that there is no association between the condition and storage behaviour. Our analysis showed a significant difference in recording behaviour of the CC-SP condition compared to the Control condition. This will reject the null hypothesis and confirms storing behaviour depends on how users are being trained. Since decision to record the passphrase is made during the training session, the more effective the training is, the less need for users to record their assigned passphrases. We also found statistically significant difference for the storing behaviour of the participants in Control compared to CC-SP w/o Cues. This confirms how the provided training can prevent users from recording their assigned passphrases.

As we provided different conditions enabled by various types training, the one that had less number of users recording their passphrase, was the condition that was enabled with two implicit learning mechanisms, CC and SP; that is, CC-SP. The less number of participants who recorded their passphrases, confirms the effectiveness of the training for this condition. It can be an indication that the designed training made them confident enough to not to record their passphrase whereas the participants in the Control condition, had such a need to record their passphrase in some ways (i.e., copy-paste, screenshot, write-down). Other conditions' participants who received some kind of training had less number of participants who record their passphrase compared to the Control condition, confirming that training can improve users' memorability. Although other conditions did not perform as promising as CC-SP, the false confidence of users prevent them from storing. This could due to an incorrect or incomplete encoding of the passphrase (displays) in their memory. Incorrect/incomplete encoding was due to inefficient cues that caused them forget what they were primed. For the CC-SP w/o Cue conditions we did not as many participants as for the Control condition who performed any recording behaviour. Although their performance was not as promising as the CC-SP condition, they did not need to store their passphrases. For the participants in this group we found some who partially recalled their passphrase, not complete recall; however, the majority were choosing words randomly which infer ineffectiveness of the training.

Training Time. The training takes at most 100 seconds, with mean login time of 64 seconds. Given improved authentication success rate, it is one time training while if users keep forgetting their system-assigned passphrases, the time they need to spend to reset their passphrase can go over 100 seconds. Moreover, organizations for which there are no alternatives, such as banks, employer, or university, tend to have stronger password composition policies. They may be helping users memorize stronger passwords by forcing them to choose a long, complex password. If such a secure password comes with a training of 100 seconds users have to go through it.

Login Time. We also hypothesized login time will be different across conditions depending on the training and/or login cues. The null hypothesis assumed the distribution of the login times are equal for all conditions. Our analysis showed statistical significant differences between conditions, confirming dependency between the provided training/login cues and login time. Effectiveness of training and login cue can decrease the required time to login.

Authentication Success Rate. The null hypothesis that we claim for the purpose of dependency between the condition and success rate, assumes that there is no association between the condition and login success rates. Evaluating login success rates for different login sessions confirmed existence of statistical differences across the conditions. This confirms how users' memories are triggered differently given the provided training and/or login cues. With CC-SP having the highest success rate compared to the other conditions, our analysis showed this condition outperforms the other conditions in terms of different metrics we considered. This implies that depending on the type of training and login cues, users' memories are triggered differently resulting in different performance.

Implicitly Reinforced Passphrases Advantages. A high level comparison of Implicitly Reinforced Passphrases with system-assigned passphrases confirms several memorability and security advantages for the proposed approach. In terms of usability, it decreases memorability burden, physical efforts, and has Infrequent errors. With regards to security benefits, Implicitly Reinforced Passphrases will provide resilience to phishing attacks, which is one of the most important attacks to be considered for authentication schemes given the ever-increasing credential theft attacks through phishing.

Implicit Employment of Memory. For indirect implicit learning-based authentication, we took advantage of CC along with another cognitive paradigm, SP. We found that with combination of these two paradigms, users can better memorize system-assigned passphrases.

We conducted our study for seven different conditions. Our results confirm our proposed approach provides improved memorability. It is worth noting that users are explicitly asked to memorize the words, which may decrease the implicit nature of the information learnt (whereas for Tacit Secrets they were not provided with any instruction to memorize anything).

In summary, the main advantages of the proposed approach, considering the condition that outperforms other conditions, CC-SP, over system-assigned passwords or PINs are: (1) improved memorability, (2) reduction in input errors, and (3) phishing resistance. CC-SP complicates phishing attacks, as the adversary would need to collect each target user's 4 displays to launch a credible attack. If comparing to a user-chosen passwords or PINs, there are even more advantages: (4) resilience to leaks from other verifiers (i.e., password leaks), (5) unlinkability (authentication information from colluding verifiers cannot be used to link the identity), and (6) negligible risk of (throttled) online attacks. It is worth noting that according to Thomas et al. [140], phishing and leaks from other verifiers are currently two important threats that lead to credential theft.

Being solely based on user name and passwords increases fragility of authentication approaches to several data breaches. Increasing amount of sensitive data (e.g., financial records, social networks) being stored in the cloud make it more demanding for security. While users different account are interrelated through emails or other information, compromising one account can jeopardize other accounts. In this work, I proposed two approaches that are not only based on a simple interaction of user with system through a text-based password, rather it incorporates their cognition while authenticating.

Chapter 7

Conclusions and Future Work

In this chapter, we summarize the major contributions of this dissertation and outline some avenues for future research.

7.1 Conclusions

Text-based passwords are a mainstay knowledge-based authentication scheme; thus, are targeted by researchers due to their wide spectrum of discovered vulnerabilities and shortcomings. Several proposals have been suggested in the literature to find a better solution with an accepted level of security as well as usability. However, the key for any solution to be successful, is to be accepted by users. Users will accept a technology/solution if they perceive its ease-of-use; otherwise, they are often not motivated to use it. This applies authentication schemes as well. Despite some providing a high level of security, they are not accepted by users if it is difficult to use.

For the sake of security, system-assigned secrets are the best solution as they meet the desired level of security for many systems; however, they usually suffer from low usability and users' acceptance. Users are more likely to forget them or have insecure behaviors in order to recall them. If the problems related to the usability of these secrets are resolved, they could meet security requirements of many systems. Thus, the main purpose of my research was to explore ways to alleviate the memorability burden of system-assigned secrets.

I chose to target implicit learning as a fundamental and ubiquitous process in cognition which has several interesting characteristics. For instance, implicit learning is a result of unconscious learning which puts less cognitive demand on users. Moreover, as discussed in Section 2.3, implicitly acquired knowledge is resistant to several mental disorders. I proposed two implicit learning based authentication approaches in order to enhance memorability of system-assigned secrets. One uses implicit learning directly and the other indirectly. My proposed authentication approaches will be able to relieve the memorization burden of authentication for system-assigned secrets. These approaches have the potential to be used by any system requiring the strong security guarantees offered by system-assigned secrets.

Through Tacit Secrets we used an implicit learning based task, CC, therein we made several changes to employ implicit memory as effective as possible. Through our proposed design, we included several design amendments to CC inspired by both previous studies and our pilot tests. This made the outcome of the study promising in order to use this implicitly acquired knowledge for authentication. To the best of our knowledge there has not been any previous work in cognitive psychology that has been considered such design features in order to enhance implicit process of the learning.

For Implicitly Reinforced Passphrases, we took advantage of two implicit learning based techniques to reinforce memorization of system-assigned authentication secrets. Contextual Cueing is traditionally a test with a target and distractors that are ‘T’ and ‘L’ letters. The promising results for Tacit Secrets made us to make some design changes and use some words instead of letters and ask users for finding a word which has different font than others. Thus, we first made some design changes in CC and then combined it with another technique, SP. SP as an implicit learning priming technique is traditionally used for retrieval from lexical-semantic memory wherein semantically related concepts are closely linked. To the best of our knowledge these two IL-based paradigms have been extensively studied separately.

However, by combining them we designed a new approach that is able to reinforce memory (in our case memory for system-assigned authentication secrets). This indicates that implicit learning of the provided stimuli depending on how often its selection is associated with positive versus negative reinforcement.

7.2 Future directions

Based on my results from both Tacit Secrets and Implicitly Reinforced Passphrases approaches, I believe that promising directions for future research include studies to employ implicit learning to trigger user's memory in order to have true cued-recall scenario for system-assigned authentication secrets. Using implicit learning mechanisms for authentication has room for improvement in the future.

7.2.1 Tacit Secrets

In order to have reliable learning, sufficient training for users is needed. If we can have shorter training that is still efficient, it can make use of implicit learning for current authentication schemes such as graphical passwords. Extracting some distinctive patterns related to the implicitly learnt knowledge of users can improve security of graphical passwords. Although the proposed approaches have a longer training time compared to traditional text-based passwords, there is promise for using these approaches for authentication. The design of my proposed approach for Tacit Secrets is based on previous work related to the contextual cueing paradigm. To be consistent with those studies, for the training session, I considered 15 blocks containing 16 trials. Although the learning effect is detectable after the fourth block, I stuck to the same number of blocks as previous work. It is worth further exploration to investigate if the training session can be further shortened while the learning is still effective and durable. To find this, further studies are required.

Another issue related Tacit Secrets that needs to be discussed is the fading effect of the learnt secrets. Based on my analysis, the difference between the average RT for the novel and repeated displays appears to have decreased slightly over the course of the experiment. This might imply that there is some fading of the CC effect over time. To mitigate the effects of implicit knowledge fading, a periodic training session could be seamlessly inserted during regular authentication sessions to make sure the displays used for authentication get continuously renewed as needed. But this would require further analysis. The retraining process can be done through either learning new displays during multiple testing sessions which can update the user's dataset partially, or it can be done through a new training session which updates the entire user's dataset and replaces the previously learnt displays' configurations with the newly learnt.

7.2.2 Implicitly Reinforced Passphrases

For implicit learning to be effective, the training needs to be complemented with cues; however, it is possible after a few login sessions, users do not need to have cues and authentication secrets can be recalled even without cue. This needs a long term future study to find if after a number of login sessions, without providing cues, users are able to recall their assigned passphrases. This is also interesting to study after the first training session, if users do not try any login session, for how long the knowledge is still accessible form their implicit memory.

Our study used a 24-48 hour and 7-8 day intervals to study long-term memorability. There is an interesting avenue for future work to study how long-term memorability is affected with multiple assigned passphrases recall sessions since each recall session can be also used as an opportunity for the users to refresh their memory of the assigned passphrase.

Given an effective training for these secure authentication secrets, they can be used for different systems seeking security. Due to the prevalence of mobile devices and multiple accounts that users need to manage in daily life, it is worth looking at how Implicitly

Reinforced Passphrases can be used for mobile devices. As discussed in Chapter 4, people have distinctive eye movements when CC is involved. So another future direction would be to use this approach to increase the effectiveness of behavioral biometric tools like eye movement patterns in distinguishing between different people when they input their assigned passphrases. Using the proposed approach, we can improve the joint level of security when used as part of a multi-factor authentication scheme. Although the use of eye tracking devices has not been widespread, with rapidly growing technologies it may be possible to have eye tracking tools embedded in mobile devices or computers in the near future.

To improve security of Implicitly Reinforced Passphrases, future work can be a study for evaluating if after a number of login sessions, we can train user on a new word. By adding a new display, containing a new word, through different login sessions, user learns the word and the context wherein the word is presented. After a number of exposures, this newly learnt word can be replaced by one of the users' previous passphrase words. Such a mechanism provides more security by constantly updating user's system-assigned passphrase. Although the current design provides resilience to online guessing attack, future works required to find if we can increase the keyspace. As threat of malware is a concern for security experts, increasing resilience to observation attacks is another important avenue for future work.

Previous studies have shown, producing items through saying them aloud can improve memorability [147]. This mechanism is called "production effect". Given the effectiveness of this effect, it provides another future direction to find if for Implicitly Reinforced Passphrases approach once they find the target word, they read it aloud, how it would affect memorability. It is also interesting to compare this effect with the memorization effects provided be CC and SP. Such a comparison can confirm which effect has more durability and effectiveness. Over the years, many user authentication technologies have been designed and deployed on security-critical systems. Among those, "what you know" forms of authentication; that is, passwords or PINs, are still the dominant manner, mainly because of their familiarity and low implementation and deployment costs. However, if they are user-chosen usually suffer from low security. In this work, I studied memorability of system-assigned passphrases, focusing on some implicit memory techniques that were traditionally applied for testing implicit memory and learning of different perceptual and motor skill tasks. To investigate ways of improving memorability, I applied some cognitive paradigms on system-assigned authentication secrets, and studied their impacts on memorability. I used CC and designed Tacit Secrets, which trained users on system-assigned secrets. The results, not surprisingly, suggests that the implicit memory can improve memorability of system-assigned secrets. For indirect implicit learning-based authentication approach, Implicitly Reinforced Passphrase, my findings lead me to a conclusion, while different implicit memory techniques can reinforce memorability of system-assigned secrets, they may not be equally effective under all circumstances, they do show promise in certain cases and warrant a more focused study. These findings shed light on a promising research direction to leverage humans' cognitive ability through cues and interaction in gaining high memorability for system-assigned authentication secrets.

So it would be interesting to evaluate effectiveness of these techniques on different authentication approaches such as graphical passwords, system-assigned PINs, or challenge-response schemes. It would also make a deeper investigation to understand the impact of these memory techniques and user interaction in improving the memorability of system-assigned authentication secrets for the people with different cognitive limitations.

References

[1] H. Bojinov, D. Sanchez, P. J. Reber, D. Boneh, and P. Lincoln, “Neuroscience meets cryptography: Designing crypto primitives secure against rubber hose attacks,” in *USENIX Security Symposium*, pp. 129–141, 2012.

[2] C. Castelluccia, M. Duermuth, M. Golla, and F. Deniz, “Towards implicit visual memory-based authentication,” in *Network and Distributed System Security Symposium (NDSS)*, (San Diego, United States), ISOC, Feb. 2017.

[3] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano, “The quest to replace passwords: A framework for comparative evaluation of web authentication schemes,” in *2012 IEEE Symposium on Security and Privacy*, pp. 553–567, May 2012.

[4] B. Ives, M. H. Olson, and J. J. Baroudi, “The measurement of user information satisfaction,” *Communications of the ACM*, vol. 26, no. 10, pp. 785–793, 1983.

[5] J. Johansson, “The great debates: Pass phrases vs. passwords,” *Security Management Ocotber*, 2004.

[6] R. Veras, C. Collins, and J. Thorpe, “On semantic patterns of passwords and their security impact,” in *NDSS*, 2014.

[7] W. Melicher, B. Ur, S. M. Segreti, S. Komanduri, L. Bauer, N. Christin, and L. F. Cranor, “Fast, lean, and accurate: Modeling password guessability using neural networks,” in *25th USENIX Security Symposium*, pp. 175–191, 2016.

[8] A. Das, J. Bonneau, M. Caesar, N. Borisov, and X. Wang, “The tangled web of password reuse,” in *NDSS*, vol. 14, pp. 23–26, 2014.

[9] T. Hunt, “;́–have i been pwned?,” 2017. Available at: https://haveibeenpwned.com/, last accessed May 26, 2017.

[10] D. Wang, Z. Zhang, P. Wang, J. Yan, and X. Huang, “Targeted online password guessing: An underestimated threat,” in *ACM CCS*, pp. 1242–1254, 2016.

[11] A. Chaabane, G. Acs, and M. A. Kaafar, “You Are What You Like! Information Leakage Through Users’ Interests,” in *Proc. Annual Network and Distributed System Security Symposium (NDSS)*, (San Diego, United States), Feb. 2012.

[12] J. Bonneau, E. Bursztein, I. Caron, R. Jackson, and M. Williamson, “Secrets, lies, and account recovery: Lessons from the use of personal knowledge questions at google,” in *Proceedings of the 24th International Conference on World Wide Web*, WWW ’15, (New York, NY, USA), pp. 141–150, ACM, 2015.

[13] D. V. Klein, "Foiling the cracker: A survey of, and improvements to, password security," in *Proceedings of the 2nd USENIX Security Workshop*, pp. 5–14, 1990.

[14] M. Zviran and W. J. Haga, "Password security: an empirical study," *Journal of Management Information Systems*, vol. 15, no. 4, pp. 161–185, 1999.

[15] A. Greenberg, "Hack brief: Password manager lastpass got breached hard," 2015. https://www.wired.com/2015/06/hack-brief-password-manager-lastpass-got-breached-hard/, accessed May 30, 2017.

[16] J. Siegrist, "Security update for the lastpass extension," 2017. https://blog.lastpass.com/2017/03/security-update-for-the-lastpass-extension.html/, accessed May 30, 2017.

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

[18] E. C. Merrill, F. A. Conners, Y. Yang, and D. Weathington, "The acquisition of contextual cueing effects by persons with and without intellectual disability," *Research in Developmental Disabilities*, vol. 35, no. 10, pp. 2341 – 2351, 2014.

[19] J. H. H. Jr., D. V. Howard, K. C. Japikse, and G. F. Eden, "Dyslexics are impaired on implicit higher-order sequence learning, but not on implicit spatial context learning," *Neuropsychologia*, vol. 44, no. 7, pp. 1131 – 1144, 2006.

[20] G. Jiménez-Fernández, J. Vaquero, L. Jiménez, and S. Defior, "Dyslexic children show deficits in implicit sequence learning, but not in explicit sequence learning or contextual cueing," *Annals of Dyslexia*, vol. 61, no. 1, pp. 85–110, 2011.

[21] P. G. Nestor, S. Han, M. Niznikiewicz, D. Salisbury, K. Spencer, M. E. Shenton, and R. W. McCarley, "Semantic disturbance in schizophrenia and its relationship to the cognitive neuroscience of attention," *Biological psychology*, vol. 57, no. 1, pp. 23–46, 2001.

[22] M. Spitzer, U. Braun, L. Hermle, and S. Maier, "Associative semantic network dysfunction in thought-disordered schizophrenic patients: direct evidence from indirect semantic priming," *Biological psychiatry*, vol. 34, no. 12, pp. 864–877, 1993.

[23] M. Kiefer, U. Martens, M. Weisbrod, L. Hermle, and M. Spitzer, "Increased unconscious semantic activation in schizophrenia patients with formal thought disorder," *Schizophrenia Research*, vol. 114, no. 1, pp. 79–83, 2009.

[24] A. Adams and M. A. Sasse, "Users are not the enemy," *Communications of the ACM*, vol. 42, no. 12, pp. 40–46, 1999.

[25] A. S. Reber, "Implicit learning and tacit knowledge.," *Journal of Experimental Psychology: General*, 1989.

[26] A. Buchner and M. C. Steffens, “Simultaneous learning of different regularities in sequence learning tasks: limits and characteristics,” *Psychological Research*, vol. 65, no. 2, pp. 71–80, 2001.

[27] V. Schmidtke and H. Heuer, “Task integration as a factor in secondary-task effects on sequence learning,” *Psychological Research*, vol. 60, no. 1-2, pp. 53–71, 1997.

[28] D. Smith, “Survivors of serious head injury can learn implicitly,” 2002. Available at: http://www.apa.org/monitor/mar02/survivors.aspx.

[29] M. Zellin, A. von Mühlenen, H. Müller, and M. Conci, “Long-term adaptation to change in implicit contextual learning,” *Psychonomic Bulletin and Review*, vol. 21, no. 4, pp. 1073–1079, 2014.

[30] A. Goujon and J. Fagot, “Learning of spatial statistics in nonhuman primates: Contextual cueing in baboons (papio papio),” *Behavioural Brain Research*, vol. 247, pp. 101 – 109, 2013.

[31] H. Bojinov, D. Sanchez, P. Reber, D. Boneh, and P. Lincoln, “Neuroscience meets cryptography: Designing crypto primitives secure against rubber hose attacks,” in *21st USENIX Security Symposium*, (Bellevue, WA), pp. 129–141, 2012.

[32] J. Carroll, *Human cognitive abilities : a survey of factor-analytic studies*. Cambridge New York: Cambridge University Press, 1993.

[33] K. VanLehn, D. Bhembe, M. Chi, C. Lynch, K. Schulze, R. Shelby, L. Taylor, D. Treacy, A. Weinstein, and M. Wintersgill, “Implicit versus explicit learning of strategies in a non-procedural cognitive skill,” in *Intelligent Tutoring Systems* (J. Lester, R. Vicari, and F. Paraguaçu, eds.), vol. 3220 of *Lecture Notes in Computer Science*, pp. 521–530, Springer Berlin Heidelberg, 2004.

[34] J. Sweller, J. v. M. Jeroen, and G. P. Fred, “Cognitive architecture and instructional design,” *Educational Psychology Review*, vol. 10, no. 3, pp. 251–296, 1998.

[35] R. C. Atkinson and R. Shiffrin, “Human memory: A proposed system and its control processes1,” vol. 2 of *Psychology of Learning and Motivation*, pp. 89 – 195, Academic Press, 1968.

[36] M. P. Driscoll and M. P. Driscoll, “Psychology of learning for instruction,” 2005.

[37] M. A. Stadler and P. A. Frensch, *Handbook of implicit learning*. CA: Sage: Thousand Oaks, 1998.

[38] A. Lleras and A. Von Mühlenen, “Spatial context and top-down strategies in visual search,” *Spatial vision*, vol. 17, no. 4-5, pp. 465–482, 2004.

[39] E. Ziori and Z. Dienes, “The time course of implicit and explicit concept learning,” *Consciousness and Cognition*, vol. 21, no. 1, pp. 204 – 216, 2012.

[40] A. S. Reber, “Implicit learning of artificial grammars,” *Journal of verbal learning and verbal behavior*, vol. 6, no. 6, pp. 855–863, 1967.

[41] K. M. Petersson, C. Forkstam, and M. Ingvar, "Artificial syntactic violations activate broca's region," *Cognitive Science*, vol. 28, no. 3, pp. 383–407, 2004.

[42] M. J. Nissen and P. Bullemer, "Attentional requirements of learning: Evidence from performance measures," *Cognitive Psychology*, vol. 19, no. 1, pp. 1–32, 1987.

[43] I. Biederman, "Perceiving real-world scenes," *Science*, vol. 177, no. 4043, pp. 77–80, 1972.

[44] E. Oudman, S. V. der Stigchel, A. J. Wester, R. P. Kessels, and A. Postma, "Intact memory for implicit contextual information in korsakoff's amnesia," *Neuropsychologia*, vol. 49, no. 10, pp. 2848 – 2855, 2011.

[45] M. M. Chun and Y. Jiang, "Contextual cueing: Implicit learning and memory of visual context guides spatial attention," *Cognitive Psychology*, 1998.

[46] A. C. Smyth and D. R. Shanks, "Awareness in contextual cuing with extended and concurrent explicit tests.," *Memory & cognition*, vol. 36, no. 2, pp. 403–415, 2008.

[47] Y. Jiang, J.-H. Song, and A. Rigas, "High-capacity spatial contextual memory," *Psychonomic Bulletin and Review*, vol. 12, no. 3, pp. 524–529, 2005.

[48] A. Kourkoulou, S. Leekam, and J. Findlay, "Implicit learning of local context in autism spectrum disorder," *Journal of Autism and Developmental Disorders*, vol. 42, no. 2, pp. 244–256, 2012.

[49] D. Lamy, A. Goshen-Kosover, N. Aviani, H. Harari, and H. Levkovitz, "Implicit memory for spatial context in depression and schizophrenia.," *Journal of abnormal psychology*, vol. 117, pp. 954–61, Nov. 2008.

[50] C. J. Vaidya, M. Huger, D. V. Howard, and J. H. Howard, "Developmental differences in implicit learning of spatial context.," *Neuropsychology*, vol. 21, no. 4, pp. 497–506, 2007.

[51] M. M. Chun and Y. Jiang, "Implicit, long-term spatial contextual memory," *Journal of experimental psychology. Learning, memory, and cognition*, vol. 29, no. 2, pp. 224–234, 2003.

[52] J. Duncan and G. W. Humphreys, "Visual search and stimulus similarity," *Psychological review*, vol. 96, no. 3, pp. 433–458, 1989.

[53] M. Pomplun, "Saccadic selectivity in complex visual search displays," *Vision Research*, vol. 46, no. 12, pp. 1886 – 1900, 2006.

[54] J. Katz and J. Fodor, "The structure of a semantic theory," *Language*, vol. 39, pp. 170–210, 1963.

[55] T. McNamara, *Semantic priming : perspectives from memory and word recognition*. New York: Psychology Press, 2005.

[56] D. E. Meyer and R. W. Schvaneveldt, "Facilitation in recognizing pairs of words: Evidence of a dependence between retrieval operations," *Journal of Experimental Psychology*, vol. 90, no. 2, p. 227, 1971.

[57] J. H. Neely, "Semantic Priming and Retrieval from Lexical Memory: Roles of Inhibitionless Spreading Activation and Limited-Capacity Attention," vol. 106, no. 3, pp. 226–254, 1977.

[58] K. McRae and S. Boisvert, "Automatic semantic similarity priming," *Journal of Experimental Psychology*, vol. 24, no. 3, p. 558, 1998.

[59] C. Herley and P. V. Oorschot, "A research agenda acknowledging the persistence of passwords," *IEEE Security Privacy*, vol. 10, pp. 28–36, Jan 2012.

[60] J. Yan, A. Blackwell, R. Anderson, and A. Grant, "Password memorability and security: Empirical results," *IEEE Security and Privacy*, vol. 2, pp. 25–31, Sept. 2004.

[61] F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS Q.*, vol. 13, pp. 319–340, Sept. 1989.

[62] K.-P. L. Vu, R. W. Proctor, A. Bhargav-Spantzel, B.-L. B. Tai, J. Cook, and E. Eugene Schultz, "Improving password security and memorability to protect personal and organizational information," *Int. J. Hum.-Comput. Stud.*, vol. 65, pp. 744–757, Aug. 2007.

[63] M. Keith, B. Shao, and P. J. Steinbart, "The usability of passphrases for authentication: An empirical field study," *International Journal of Human-Computer Studies*, vol. 65, no. 1, pp. 17–28, 2007.

[64] R. Shay, P. G. Kelley, S. Komanduri, M. L. Mazurek, B. Ur, T. Vidas, L. Bauer, N. Christin, and L. F. Cranor, "Correct horse battery staple: Exploring the usability of system-assigned passphrases," in *Symposium on Usable Privacy and Security (SOUPS)*, pp. 7:1–7:20, 2012.

[65] J. Bonneau and S. Schechter, "Towards reliable storage of 56-bit secrets in human memory," in *USENIX Security Symposium*, pp. 607–623, 2014.

[66] W. E. Burr, D. F. Dodson, E. M. Newton, R. A. Perlner, W. T. Polk, S. Gupta, and E. A. Nabbus, "Sp 800-63-1. electronic authentication guideline," tech. rep., Gaithersburg, MD, United States, 2011.

[67] L. O'Gorman, "Comparing passwords, tokens, and biometrics for user authentication," *Proceedings of the IEEE*, vol. 91, pp. 2021–2040, Dec 2003.

[68] A. K. Jain, A. Ross, and S. Pankanti, "Biometrics: a tool for information security," *IEEE Transactions on Information Forensics and Security*, vol. 1, pp. 125–143, June 2006.

[69] J. Brainard, A. Juels, R. L. Rivest, M. Szydlo, and M. Yung, "Fourth-factor authentication: Somebody you know," in *Proceedings of the 13th ACM Conference on Computer and Communications Security*, CCS '06, (New York, NY, USA), pp. 168–178, ACM, 2006.

[70] L. Cranor, *Security and usability : designing secure systems that people can use*. Beijing Farnham Sebastopol, CA: O'Reilly, 2005.

[71] B. Sathish and P. Venkataram, “Transaction based authentication scheme for mobile communication: A cognitive agent based approach,” in *Parallel and Distributed Processing Symposium, 2007. IPDPS 2007. IEEE International*, pp. 1–8, March 2007.

[72] A. De Luca, A. Hang, F. Brudy, C. Lindner, and H. Hussmann, “Touch me once and i know it’s you!: Implicit authentication based on touch screen patterns,” in *SIGCHI Conference on Human Factors in Computing Systems*, CHI ’12, (New York, NY, USA), pp. 987–996, ACM, 2012.

[73] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, “The design and analysis of graphical passwords,” in *8th Conference on USENIX Security Symposium - Volume 8*, SSYM’99, (Berkeley, CA, USA), pp. 1–1, 1999.

[74] D. J. Sanchez, E. W. Gobel, and P. J. Reber, “Performing the unexplainable: implicit task performance reveals individually reliable sequence learning without explicit knowledge.,” *Psychonomic bulletin and review*, vol. 17, no. 6, pp. 790–796, 2010.

[75] T. Denning, K. Bowers, M. van Dijk, and A. Juels, “Exploring implicit memory for painless password recovery,” in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI ’11, (New York, NY, USA), pp. 2615–2618, ACM, 2011.

[76] S. Eberz, K. B. Rasmussen, V. Lenders, and I. Martinovic, “Preventing lunchtime attacks: Fighting insider threats with eye movement biometrics,” in *The Network and Distributed System Security Symposium (NDSS)*, February 2015.

[77] A. Rao, B. Jha, and G. Kini, “Effect of grammar on security of long passwords,” in *Proceedings of the third ACM conference on Data and application security and Privacy*, pp. 317–324, ACM, 2013.

[78] S. N. Porter, “A password extension for improved human factors,” *Computers & Security*, vol. 1, no. 1, pp. 54–56, 1982.

[79] M. Keith, B. Shao, and P. J. Steinbart, “The usability of passphrases for authentication: An empirical field study,” *Int. J. Hum.-Comput. Stud.*, vol. 65, pp. 17–28, Jan. 2007.

[80] J. Bonneau and E. Shutova, “Linguistic properties of multi-word passphrases,” in *Proceedings of the 16th International Conference on Financial Cryptography and Data Security*, FC’12, (Berlin, Heidelberg), pp. 1–12, Springer-Verlag, 2012.

[81] T. A. Salthouse, “Perceptual, cognitive, and motoric aspects of transcription typing.,” *Psychological bulletin*, vol. 99, no. 3, p. 303, 1986.

[82] G. V. Bard, “Spelling-error tolerant, order-independent pass-phrases via the damerau-levenshtein string-edit distance metric,” in *Proceedings of the Fifth Australasian Symposium on ACSW Frontiers - Volume 68*, ACSW ’07, (Darlinghurst, Australia, Australia), pp. 117–124, Australian Computer Society, Inc., 2007.

[83] A. Mehler and S. Skiena, “Improving usability through password-corrective hashing,” in *Proceedings of the 13th International Conference on String Processing and Information Retrieval*, SPIRE’06, (Berlin, Heidelberg), pp. 193–204, Springer-Verlag, 2006.

[84] A. Perrig and D. Song, “Hash visualization: A new technique to improve real-world security,” in *International Workshop on Cryptographic Techniques and E-Commerce*, pp. 131–138, 1999.

[85] C. Kuo, S. Romanosky, and L. F. Cranor, “Human selection of mnemonic phrase-based passwords,” in *Proceedings of the Second Symposium on Usable Privacy and Security*, SOUPS ’06, (New York, NY, USA), pp. 67–78, ACM, 2006.

[86] M. Savva, A. X. Chang, C. D. Manning, and P. Hanrahan, “TransPhoner: Automated Mnemonic Keyword Generation,” pp. 3725–3734, 2014.

[87] R. C. Atkinson and M. R. Raugh, “An application of the mnemonic keyword method to the acquisition of a Russian vocabulary,” *Journal of Experimental Psychology:Human Learning and Memory*, vol. 1, no. 2, p. 126, 1975.

[88] N. C. Ellis and A. Beaton, “Psycholinguistic determinants of foreign language vocabulary learning,” *Language Learning*, vol. 43, no. 4, pp. 559–617, 1993.

[89] O. Anonthanasap, M. Ketna, and T. Leelanupab, “Automated english mnemonic keyword suggestion for learning japanese vocabulary,” in *2015 7th International Conference on Information Technology and Electrical Engineering (ICITEE)*, pp. 638–643, Oct 2015.

[90] R. Shay, S. Komanduri, A. L. Durity, P. S. Huh, M. L. Mazurek, S. M. Segreti, B. Ur, L. Bauer, N. Christin, and L. F. Cranor, “Can long passwords be secure and usable?,” in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI ’14, (New York, NY, USA), pp. 2927–2936, ACM, 2014.

[91] D. E. Meyer and R. W. Schvaneveldt, “Facilitation in recognizing pairs of words: Evidence of a dependence between retrieval operations,” *Journal of Experimental Psychology*, vol. 90, no. 2, p. 227, 1971.

[92] G. A. MILLER, “the Magical Number 7, Plus or Minus 2 - Some Limits on Our Capacity for Processing Information,” 1956.

[93] US Department of Defense, “Password Management Guidelines,” no. April, 1985.

[94] S. Komanduri, R. Shay, P. G. Kelley, M. L. Mazurek, L. Bauer, N. Christin, L. F. Cranor, and S. Egelman, “Of Passwords and People: Measuring the Effect of Password-Composition Policies,” *Proceedings of the 2011 annual conference on Human factors in computing systems - CHI ’11*, p. 2595, 2011.

[95] R. Shay, S. Komanduri, P. G. Kelley, P. G. Leon, M. L. Mazurek, L. Bauer, N. Christin, and L. F. Cranor, “Encountering Stronger Password Requirements: User Attitudes and Behaviors,” *Proceedings of the Sixth Symposium on Usable Privacy and Security - SOUPS ’10*, p. 1, 2010.

[96] M. Bishop, “Password management,” 1991.

[97] S. Jeyaraman and U. Topkara, “Have the cake and eat it too - Infusing usability into text-password based authentication systems,” *Proceedings - Annual Computer Security Applications Conference, ACSAC*, vol. 2005, pp. 473–482, 2005.

[98] H. Crawford and J. Aycock, “Kwyjibo: automatic domain name generation,” *Software: Practice and Experience*, vol. 38, no. 14, pp. 1561–1567, 2008.

[99] M. N. Al-Ameen, M. Wright, and S. Scielzo, “Towards making random passwords memorable: Leveraging users’ cognitive ability through multiple cues,” in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, CHI ’15, (New York, NY, USA), pp. 2315–2324, ACM, 2015.

[100] M. S. Turan, E. Barker, W. Burr, and L. Chen, “Recommendation for Password-Based Key Derivation Part 1 : Storage Applications,” no. December, 2010.

[101] W. E. Burr, D. F. Dodson, E. M. Newton, R. A. Perlner, W. T. Polk, S. Gupta, and E. A. Nabbus, “Sp 800-63-1. electronic authentication guideline,” tech. rep., Gaithersburg, MD, United States, 2011.

[102] M. S. Turan, E. B. Barker, W. E. Burr, and L. Chen, “Sp 800-132. recommendation for password-based key derivation: Part 1: Storage applications,” 2010.

[103] M. Keith, B. Shao, and P. Steinbart, “A behavioral analysis of passphrase design and effectiveness,” *Journal of the Association for Information Systems*, vol. 10, no. 2, 2009.

[104] Y. Spector and J. Ginzberg, “Pass-sentence-a new approach to computer code,” *Computers & Security*, vol. 13, no. 2, pp. 145–160, 1994.

[105] M. Zviran and W. J. Haga, “A comparison of password techniques for multilevel authentication mechanisms,” *The Computer Journal*, vol. 36, no. 3, pp. 227–237, 1993.

[106] J. Yan, A. Blackwell, R. Anderson, and A. Grant, “Password memorability and security: Empirical results,” *IEEE Security & Privacy*, vol. 2, no. 5, pp. 25–31, 2004.

[107] J. Bonneau and E. Shutova, “Linguistic properties of multi-word passphrases,” in *International Conference on Financial Cryptography and Data Security*, pp. 1–12, Springer, 2012.

[108] J. Bonneau, “The science of guessing: analyzing an anonymized corpus of 70 million passwords,” in *Security and Privacy (SP), 2012 IEEE Symposium on*, pp. 538–552, IEEE, 2012.

[109] R. Munroe, “xkcd: Password strength,” 2012.

[110] M. N. Al-Ameen, M. Wright, and S. Scielzo, “Towards making random passwords memorable: Leveraging users’ cognitive ability through multiple cues,” in *ACM Conference on Human Factors in Computing Systems (CHI)*, pp. 2315–2324, 2015.

[111] J. Clark and U. Hengartner, “Panic passwords: Authenticating under duress,” in *Proceedings of the 3rd Conference on Hot Topics in Security*, HOTSEC’08, (Berkeley, CA, USA), pp. 8:1–8:6, USENIX Association, 2008.

[112] P. Gupta and D. Gao, “Fighting coercion attacks in key generation using skin conductance,” USENIX Security’10, (Berkeley, CA, USA), pp. 30–35, USENIX Association, 2010.

[113] P. Gupta, X. Ding, and D. Gao, "Coercion resistance in authentication responsibility shifting," in *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security*, ASIACCS '12, (New York, NY, USA), pp. 97–98, ACM, 2012.

[114] T. Okamoto, "Receipt-free electronic voting schemes for large scale elections," in *Security Protocols* (B. Christianson, B. Crispo, M. Lomas, and M. Roe, eds.), vol. 1361 of *Lecture Notes in Computer Science*, pp. 25–35, Springer Berlin Heidelberg, 1998.

[115] R. Canetti, C. Dwork, M. Naor, and R. Ostrovsky, "Deniable encryption," in *Advances in Cryptology — CRYPTO '97* (J. Kaliski, BurtonS., ed.), vol. 1294 of *Lecture Notes in Computer Science*, pp. 90–104, Springer Berlin Heidelberg, 1997.

[116] D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Commun. ACM*, vol. 24, pp. 84–90, Feb. 1981.

[117] MTurk, "Amazon mechanical turk," 2017. https://www.mturk.com/mturk/welcome.

[118] G. D. Logan, "Toward an instance theory of automatization.," *Psychological review*, vol. 95, no. 4, p. 492, 1988.

[119] J. R. Brockmole and J. M. Henderson, "Using real-world scenes as contextual cues for search," *Visual Cognition*, vol. 13, no. 1, pp. 99–108, 2006.

[120] A. Goujon, A. Didierjean, and S. Poulet, "The emergence of explicit knowledge from implicit learning," *Memory Cognition*, vol. 42, no. 2, pp. 225–236, 2014.

[121] T. Geyer, M. Zehetleitner, and H. J. Müller, "Contextual cueing of pop-out visual search: When context guides the deployment of attention.," *Journal of vision*, vol. 10, p. 20, 2010.

[122] G. Zhao, Q. Liu, J. Jiao, P. Zhou, H. Li, and H.-j. Sun, "Dual-state modulation of the contextual cueing effect: Evidence from eye movement recordings," *Journal of Vision*, vol. 12, pp. 11–11, 2012.

[123] R. Shay, P. G. Kelley, S. Komanduri, M. L. Mazurek, B. Ur, T. Vidas, L. Bauer, N. Christin, and L. F. Cranor, "Correct horse battery staple: Exploring the usability of system-assigned passphrases," in *Proceedings of the Eighth Symposium on Usable Privacy and Security*, SOUPS '12, (New York, NY, USA), pp. 7:1–7:20, ACM, 2012.

[124] Tobii, "Tobii pro tx300," 2017. Available at: https://www.tobiipro.com/product-listing/tobii-pro-tx300/, urldate=2017-10-01.

[125] D. I. Brooks, I. P. Rasmussen, and A. Hollingworth, "The nesting of search contexts within natural scenes: evidence from contextual cuing.," *Journal of experimental psychology. Human perception and performance*, vol. 36, pp. 1406–18, Dec. 2010.

[126] D. Smilek, J. T. Enns, J. D. Eastwood, and P. M. Merikle, "Relax! cognitive strategy influences visual search," *Visual Cognition*, vol. 14, no. 4-8, pp. 543–564, 2006.

[127] Y.-C. Tseng and A. Lleras, "Rewarding context accelerates implicit guidance in visual search," *Attention, Perception, Psychophysics*, vol. 75, no. 2, pp. 287–298, 2013.

[128] D. Florêncio, C. Herley, and P. C. van Oorschot, "An administrator's guide to internet password research," in *28th Large Installation System Administration Conference (LISA14)*, pp. 44–61, 2014.

[129] D. Florêncio, C. Herley, and P. C. Van Oorschot, "An administrator's guide to internet password research," in *Proceedings of the 28th USENIX Conference on Large Installation System Administration*, LISA'14, (Berkeley, CA, USA), pp. 35–52, USENIX Association, 2014.

[130] M. Stahnke, "The openssh client," *Pro OpenSSH*, pp. 69–112, 2006.

[131] M. Binder, *Encyclopedia of neuroscience*. Berlin London: Springer, 2009.

[132] B. Ur, J. Bees, S. M. Segreti, L. Bauer, N. Christin, and L. F. Cranor, "Do users' perceptions of password security match reality?," in *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pp. 3748–3760, ACM, 2016.

[133] "word2vec," 2013.

[134] J. Brooke *et al.*, "Sus-a quick and dirty usability scale," *Usability evaluation in industry*, vol. 189, no. 194, pp. 4–7, 1996.

[135] J. Sauro, "Measuring usability with the system usability scale (sus)," 2011. https://measuringu.com/sus/, accessed Sep 30, 2017.

[136] J. Bonneau, C. Herley, P. C. v. Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," in *IEEE Symposium on Security and Privacy*, pp. 553–567, 2012.

[137] J. H. Huh, H. Kim, R. B. Bobba, M. N. Bashir, and K. Beznosov, "On the memorability of system-generated pins: Can chunking help?," in *SOUPS*, pp. 197–209, 2015.

[138] P. G. Inglesant and M. A. Sasse, "The true cost of unusable password policies: password use in the wild," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 383–392, ACM, 2010.

[139] K.-P. L. Vu, R. W. Proctor, A. Bhargav-Spantzel, B.-L. B. Tai, J. Cook, and E. E. Schultz, "Improving password security and memorability to protect personal and organizational information," *International Journal of Human-Computer Studies*, vol. 65, no. 8, pp. 744–757, 2007.

[140] K. Thomas, F. Li, A. Zand, J. Barrett, J. Ranieri, L. Invernizzi, Y. Markov, O. Comanescu, V. Eranti, A. Moscicki, *et al.*, "Data breaches, phishing, or malware? understanding the risks of stolen credentials," 2017.

[141] 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*, pp. 121–130, British Computer Society, 2008.

[142] A. Wilson, A. Fern, S. Ray, and P. Tadepalli, "Multi-task reinforcement learning: A hierarchical bayesian approach," in *Proceedings of the 24th International Conference on Machine Learning*, ICML '07, (New York, NY, USA), pp. 1015–1022, ACM, 2007.

[143] B. Ur, P. G. Kelley, S. Komanduri, J. Lee, M. Maass, M. L. Mazurek, T. Passaro, R. Shay, T. Vidas, L. Bauer, *et al.*, “How does your password measure up? the effect of strength meters on password creation.,” in *USENIX Security Symposium*, pp. 65–80, 2012.

[144] S. Egelman, A. Sotirakopoulos, I. Muslukhov, K. Beznosov, and C. Herley, “Does my password go up to eleven?: the impact of password meters on password selection,” in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 2379–2388, ACM, 2013.

[145] S. Van Acker, D. Hausknecht, W. Joosen, and A. Sabelfeld, “Password meters and generators on the web: From large-scale empirical study to getting it right,” in *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy*, pp. 253–262, ACM, 2015.

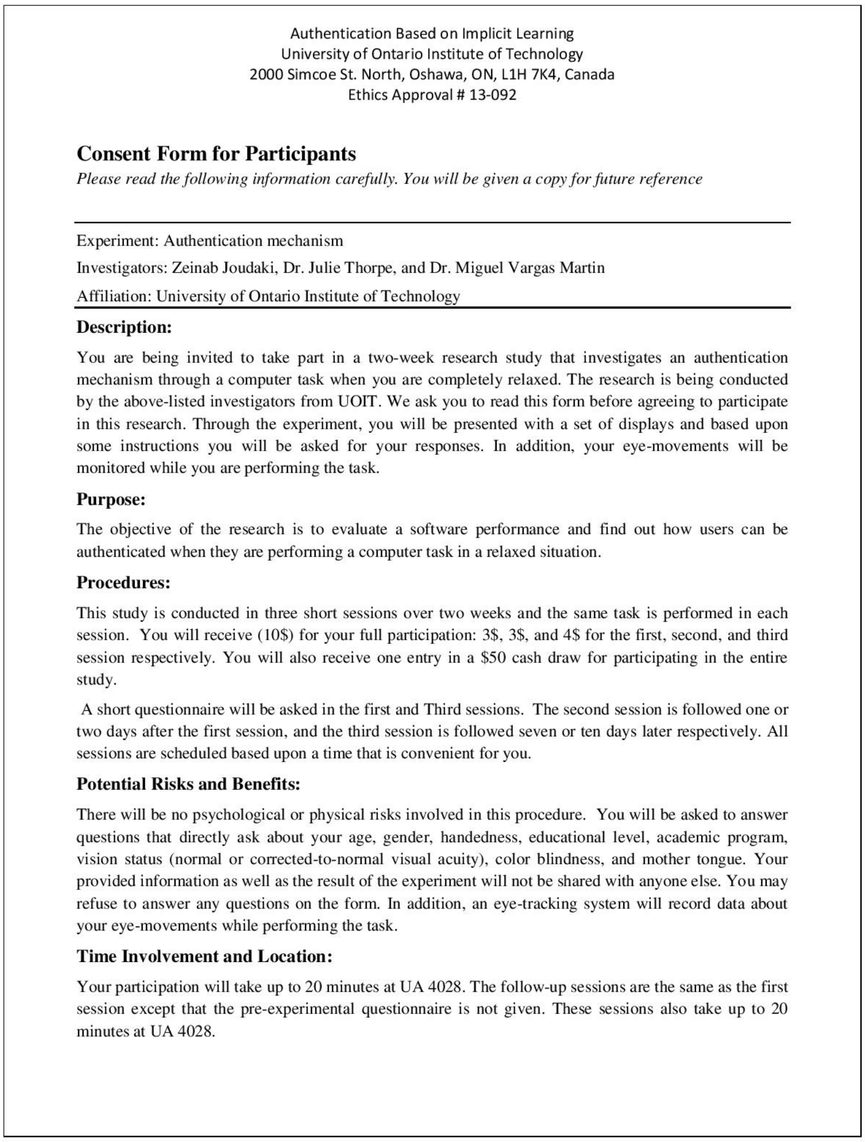
[146] A. Karole, N. Saxena, and N. Christin, “A comparative usability evaluation of traditional password managers.,” in *ICISC*, pp. 233–251, Springer, 2010.

[147] M. Icht, Y. Mama, and D. Algom, “The production effect in memory: Multiple species of distinctiveness,” *Frontiers in psychology*, vol. 5, 2014.

Appendix A

Tacit Secrets

A.1 Consent form for Tacit Secret in-lab Study



Authentication Based on Implicit Learning
University of Ontario Institute of Technology
2000 Simcoe St. North, Oshawa, ON, L1H 7K4, Canada
Ethics Approval # 13-092

Consent Form for Participants

Please read the following information carefully. You will be given a copy for future reference

Experiment: Authentication mechanism

Investigators: Zeinab Joudaki, Dr. Julie Thorpe, and Dr. Miguel Vargas Martin

Affiliation: University of Ontario Institute of Technology

Description:

You are being invited to take part in a two-week research study that investigates an authentication mechanism through a computer task when you are completely relaxed. The research is being conducted by the above-listed investigators from UOIT. We ask you to read this form before agreeing to participate in this research. Through the experiment, you will be presented with a set of displays and based upon some instructions you will be asked for your responses. In addition, your eye-movements will be monitored while you are performing the task.

Purpose:

The objective of the research is to evaluate a software performance and find out how users can be authenticated when they are performing a computer task in a relaxed situation.

Procedures:

This study is conducted in three short sessions over two weeks and the same task is performed in each session. You will receive (10$) for your full participation: 3$, 3$, and 4$ for the first, second, and third session respectively. You will also receive one entry in a $50 cash draw for participating in the entire study.

A short questionnaire will be asked in the first and Third sessions. The second session is followed one or two days after the first session, and the third session is followed seven or ten days later respectively. All sessions are scheduled based upon a time that is convenient for you.

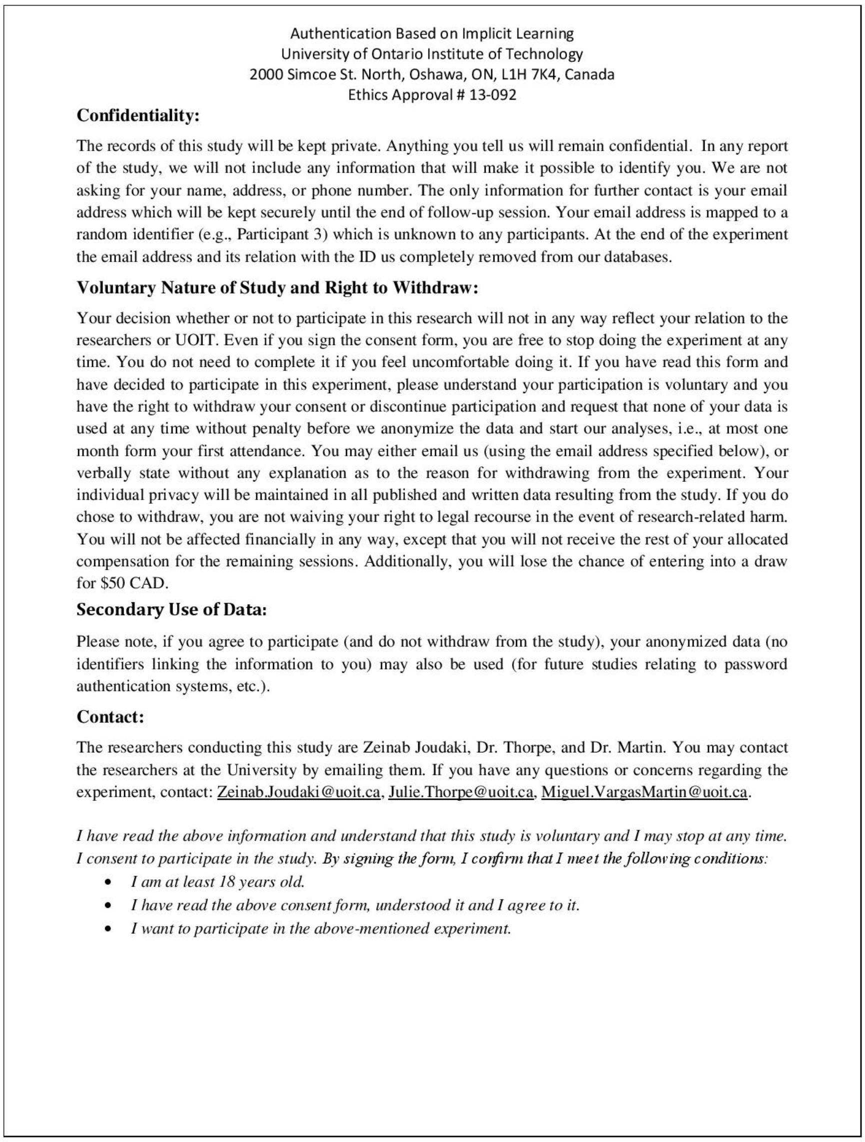
Potential Risks and Benefits:

There will be no psychological or physical risks involved in this procedure. You will be asked to answer questions that directly ask about your age, gender, handedness, educational level, academic program, vision status (normal or corrected-to-normal visual acuity), color blindness, and mother tongue. Your provided information as well as the result of the experiment will not be shared with anyone else. You may refuse to answer any questions on the form. In addition, an eye-tracking system will record data about your eye-movements while performing the task.

Time Involvement and Location:

Your participation will take up to 20 minutes at UA 4028. The follow-up sessions are the same as the first session except that the pre-experimental questionnaire is not given. These sessions also take up to 20 minutes at UA 4028.

Fig. A.1 Tacit Secrets - Consent Form (Page 1 of 3).



Authentication Based on Implicit Learning
University of Ontario Institute of Technology
2000 Simcoe St. North, Oshawa, ON, L1H 7K4, Canada
Ethics Approval # 13-092

Confidentiality:

The records of this study will be kept private. Anything you tell us will remain confidential. In any report of the study, we will not include any information that will make it possible to identify you. We are not asking for your name, address, or phone number. The only information for further contact is your email address which will be kept securely until the end of follow-up session. Your email address is mapped to a random identifier (e.g., Participant 3) which is unknown to any participants. At the end of the experiment the email address and its relation with the ID us completely removed from our databases.

Voluntary Nature of Study and Right to Withdraw:

Your decision whether or not to participate in this research will not in any way reflect your relation to the researchers or UOIT. Even if you sign the consent form, you are free to stop doing the experiment at any time. You do not need to complete it if you feel uncomfortable doing it. If you have read this form and have decided to participate in this experiment, please understand your participation is voluntary and you have the right to withdraw your consent or discontinue participation and request that none of your data is used at any time without penalty before we anonymize the data and start our analyses, i.e., at most one month form your first attendance. You may either email us (using the email address specified below), or verbally state without any explanation as to the reason for withdrawing from the experiment. Your individual privacy will be maintained in all published and written data resulting from the study. If you do chose to withdraw, you are not waiving your right to legal recourse in the event of research-related harm. You will not be affected financially in any way, except that you will not receive the rest of your allocated compensation for the remaining sessions. Additionally, you will lose the chance of entering into a draw for $50 CAD.

Secondary Use of Data:

Please note, if you agree to participate (and do not withdraw from the study), your anonymized data (no identifiers linking the information to you) may also be used (for future studies relating to password authentication systems, etc.).

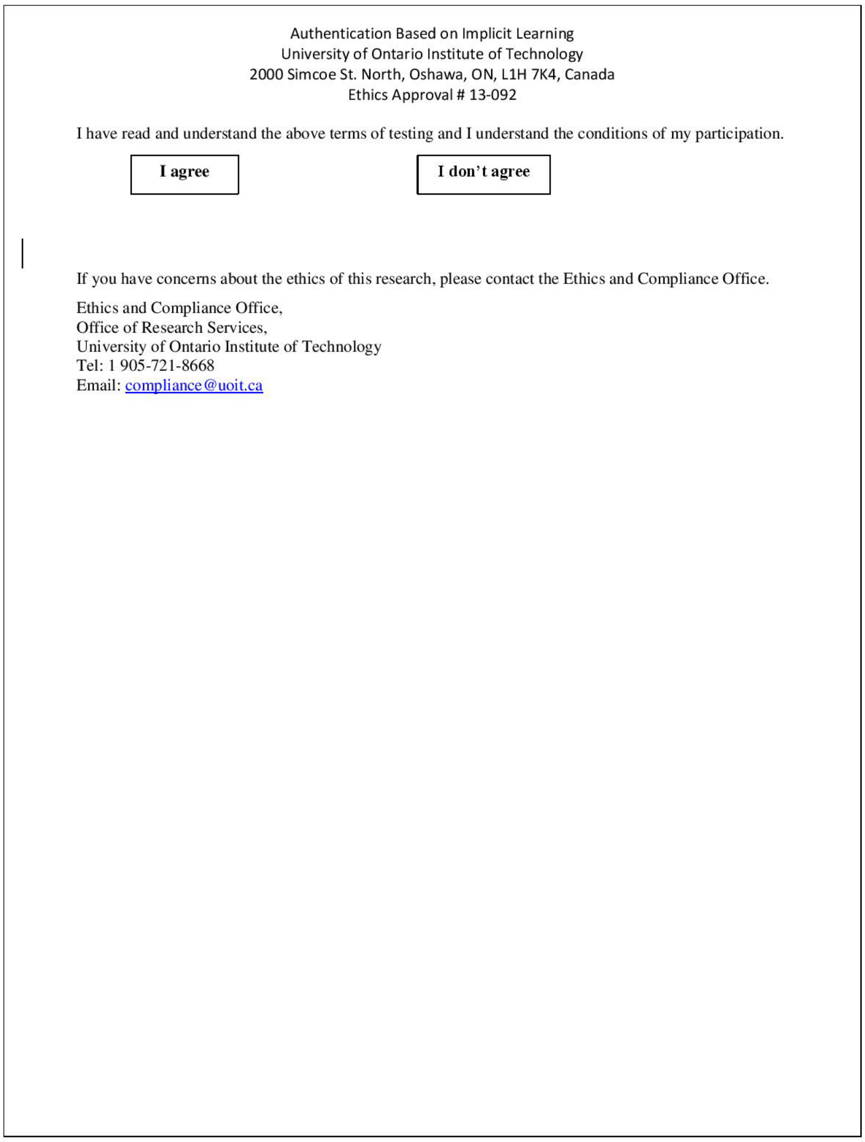
Contact:

The researchers conducting this study are Zeinab Joudaki, Dr. Thorpe, and Dr. Martin. You may contact the researchers at the University by emailing them. If you have any questions or concerns regarding the experiment, contact: Zeinab.Joudaki@uoit.ca, Julie.Thorpe@uoit.ca, Miguel.VargasMartin@uoit.ca.

I have read the above information and understand that this study is voluntary and I may stop at any time. I consent to participate in the study. By signing the form, I confirm that I meet the following conditions:

- *I am at least 18 years old.*
- *I have read the above consent form, understood it and I agree to it.*
- *I want to participate in the above-mentioned experiment.*

Fig. A.2 Tacit Secrets - Consent Form (Page 2 of 3).



Authentication Based on Implicit Learning
University of Ontario Institute of Technology
2000 Simcoe St. North, Oshawa, ON, L1H 7K4, Canada
Ethics Approval # 13-092

I have read and understand the above terms of testing and I understand the conditions of my participation.

I agree **I don't agree**

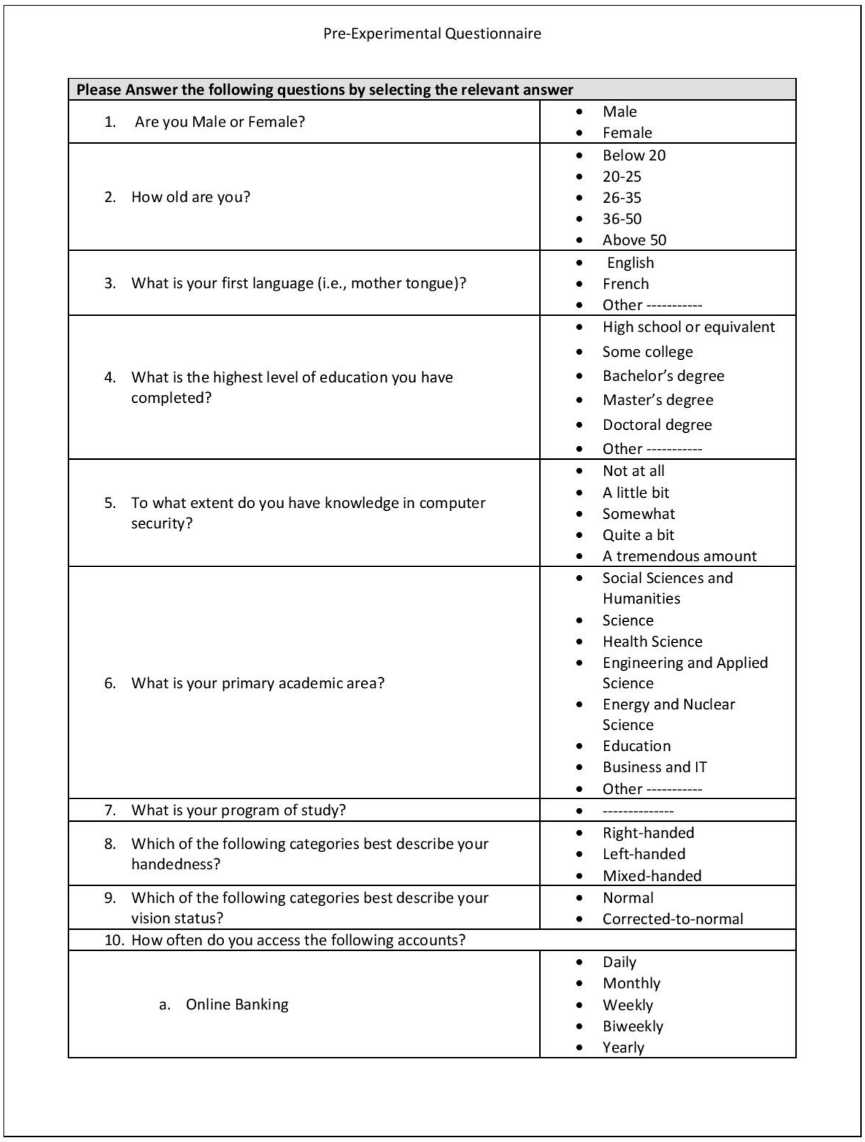
If you have concerns about the ethics of this research, please contact the Ethics and Compliance Office.

Ethics and Compliance Office,
Office of Research Services,
University of Ontario Institute of Technology
Tel: 1 905-721-8668
Email: compliance@uoit.ca

[H]

Fig. A.3 Tacit Secrets - Consent Form (Page 3 of 3).

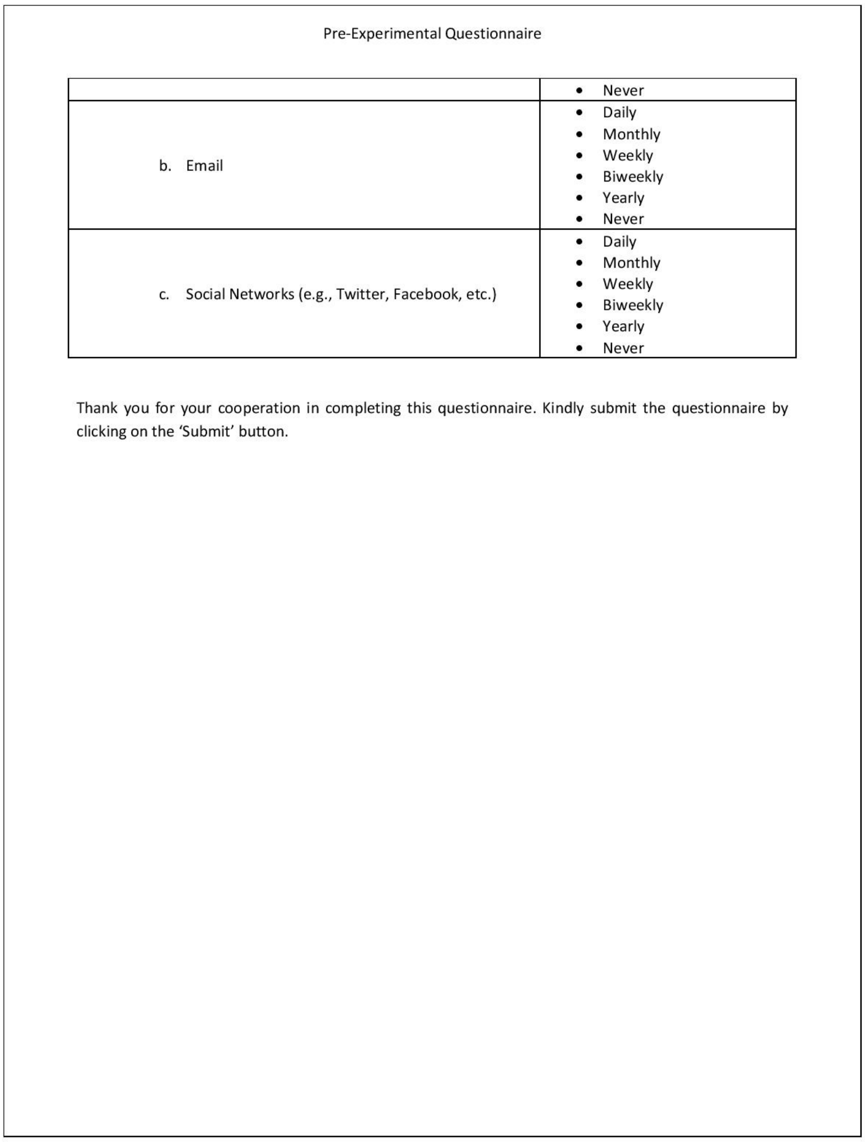
A.2 Questionnaires



Pre-Experimental Questionnaire

Please Answer the following questions by selecting the relevant answer	
1. Are you Male or Female?	• Male • Female
2. How old are you?	• Below 20 • 20-25 • 26-35 • 36-50 • Above 50
3. What is your first language (i.e., mother tongue)?	• English • French • Other -----------
4. What is the highest level of education you have completed?	• High school or equivalent • Some college • Bachelor's degree • Master's degree • Doctoral degree • Other -----------
5. To what extent do you have knowledge in computer security?	• Not at all • A little bit • Somewhat • Quite a bit • A tremendous amount
6. What is your primary academic area?	• Social Sciences and Humanities • Science • Health Science • Engineering and Applied Science • Energy and Nuclear Science • Education • Business and IT • Other -----------
7. What is your program of study?	• --------------
8. Which of the following categories best describe your handedness?	• Right-handed • Left-handed • Mixed-handed
9. Which of the following categories best describe your vision status?	• Normal • Corrected-to-normal
10. How often do you access the following accounts?	
a. Online Banking	• Daily • Monthly • Weekly • Biweekly • Yearly

Fig. A.4 Tacit Secrets - Pre-experiment questionnaire (Page 1).

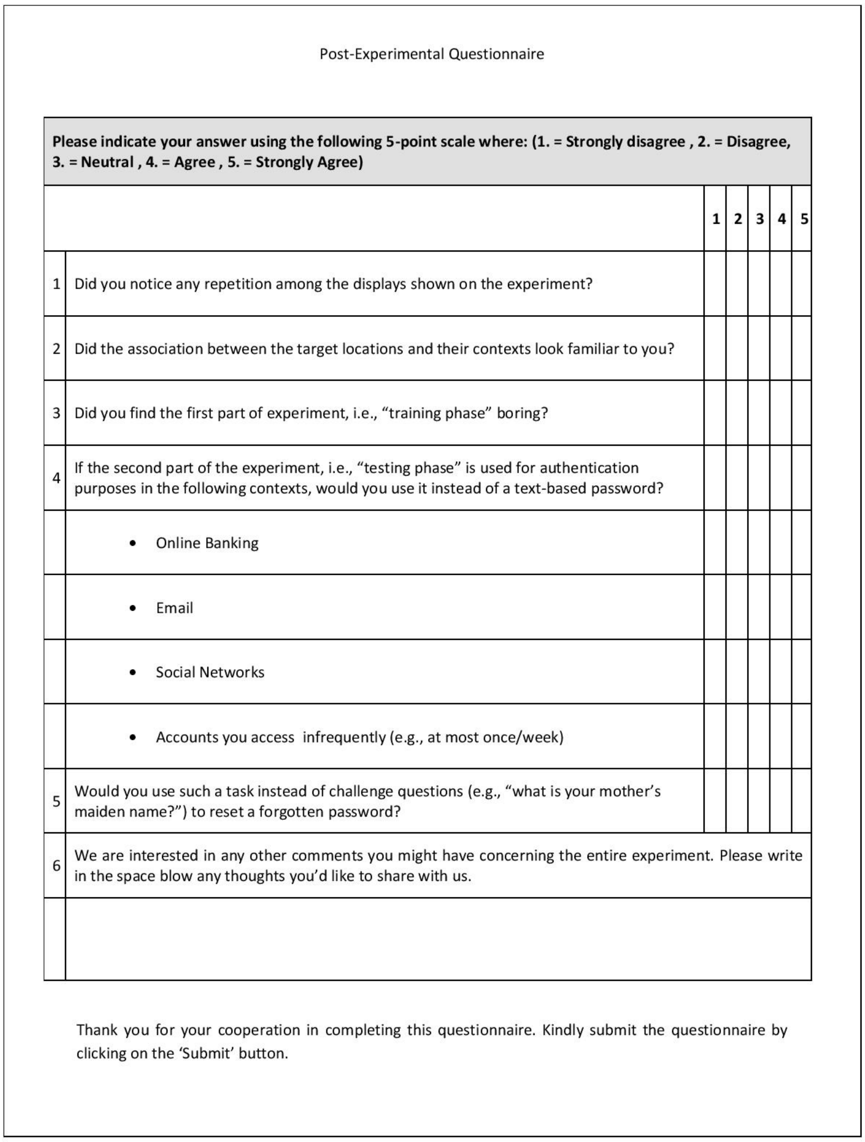


Pre-Experimental Questionnaire

	• Never
b. Email	• Daily • Monthly • Weekly • Biweekly • Yearly • Never
c. Social Networks (e.g., Twitter, Facebook, etc.)	• Daily • Monthly • Weekly • Biweekly • Yearly • Never

Thank you for your cooperation in completing this questionnaire. Kindly submit the questionnaire by clicking on the 'Submit' button.

Fig. A.5 Tacit Secrets - Pre-experiment questionnaire (Page 2).



Post-Experimental Questionnaire

Please indicate your answer using the following 5-point scale where: (1. = Strongly disagree , 2. = Disagree, 3. = Neutral , 4. = Agree , 5. = Strongly Agree)						
		1	**2**	**3**	**4**	**5**
1	Did you notice any repetition among the displays shown on the experiment?					
2	Did the association between the target locations and their contexts look familiar to you?					
3	Did you find the first part of experiment, i.e., “training phase” boring?					
4	If the second part of the experiment, i.e., “testing phase” is used for authentication purposes in the following contexts, would you use it instead of a text-based password?					
	• Online Banking					
	• Email					
	• Social Networks					
	• Accounts you access infrequently (e.g., at most once/week)					
5	Would you use such a task instead of challenge questions (e.g., “what is your mother’s maiden name?”) to reset a forgotten password?					
6	We are interested in any other comments you might have concerning the entire experiment. Please write in the space blow any thoughts you’d like to share with us.					

Thank you for your cooperation in completing this questionnaire. Kindly submit the questionnaire by clicking on the ‘Submit’ button.

Fig. A.6 Tacit Secrets - Post-experiment questionnaire (Page 1).

A.3 Screenshots of Sample Tacit Secrets displays

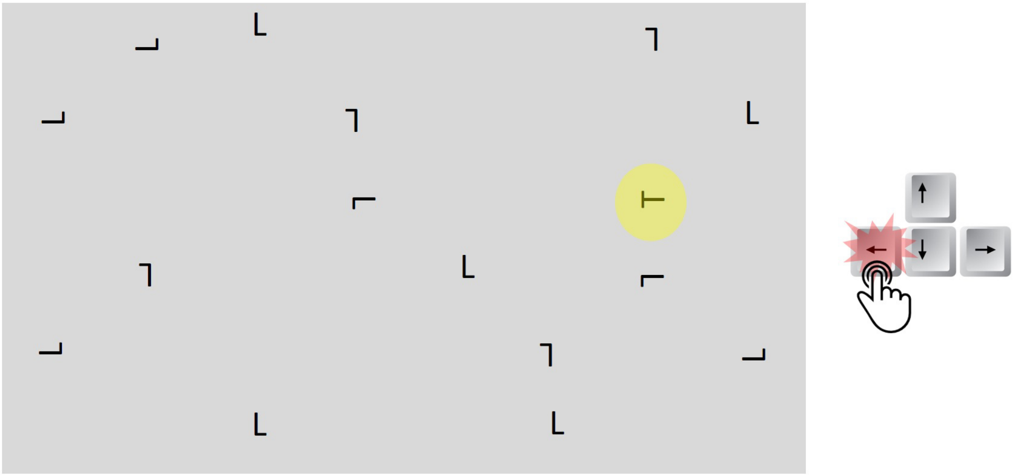


Fig. A.7 Sample display for Tacit Secrets Experiment. The target word is a ‘T’ letter which is surrounded with rotated ‘L’ letters. The user task is to find the target and press corresponding arrow key based on the target orientation.

A.4 Average and standard deviation of subjects’ RT

Subject	Type	Testing Session 1		Testing Session 2		Testing Session 3	
		avg	stdev	avg	stdev	avg	stdev
P_1	R	1,258.08	364.85			1,511.62	955.63
	N	1,647.80	533.37			1,677.76	602.66
P_2	R	1,133.90	592.20	1,183.89	393.98	1,284.73	471.38
	N	1,929.28	680.89	1,724.65	405.21	1,562.26	504.27
	R	1,390.22	297.57	1,406.84	540.05	1,005.25	416.23

Continued on next page

Table A.1 – *Continued from previous page*

Participant	Type	Testing Session 1		Testing Session 2		Testing Session 3	
		avg	stdev	avg	stdev	avg	stdev
P_3	N	1,695.85	809.91	1,666.71	453.27	1,687.80	342.36
P_4	R	1,198.43	755.43	1,279.77	608.80	1,323.59	623.82
	N	1,818.33	768.74	1,737.65	535.20	1,625.82	565.24
P_5	R	1,250.93	623.99	1,286.47	326.88	1,148.37	271.31
	N	1,902.46	359.86	1,703.76	444.22	1,573.81	412.89
P_6	R	1,239.67	287.06	1,193.38	204.00	1,018.12	233.96
	N	1,841.48	301.91	1,530.41	240.80	1,548.46	241.54
P_7	R	1,082.64	733.18				
	N	1,781.66	770.11				
P_8	R	1,164.36	540.97	1,122.39	355.95	1,412.97	637.46
	N	1,721.10	658.50	1,687.98	319.33	1,707.94	622.88
P_9	R	1,175.88	392.14	1,130.83	291.66	1,248.10	225.52
	N	1,672.89	402.24	1,827.25	627.35	1,437.24	352.79
P_{10}	R	1,142.42	454.35	1,086.05	485.72	1,069.03	407.53
	N	1,642.41	630.86	1,992.64	510.68	1,371.78	397.28
P_{11}	R	1,008.85	272.82	1,056.70	366.31	1,203.74	350.20
	N	1,799.40	379.17	1,782.05	518.54	1,433.73	463.73
P_{12}	R	1,201.50	335.48	1,400.18	550.16	1,367.09	524.21
	N	1,962.64	268.19	1,541.40	722.20	1,843.47	585.41
P_{13}	R	1,108.33	239.54	1,179.50	366.70	1,433.38	479.57
	N	2,190.50	531.42	1,865.54	520.68	1,698.88	461.10

Continued on next page

Table A.1 – *Continued from previous page*

Participant	Type	Testing Session 1		Testing Session 2		Testing Session 3	
		avg	stdev	avg	stdev	avg	stdev
P_{14}	R	1,503.23	324.44	1,309.91	599.32	1,419.65	716.87
	N	1,622.98	453.52	1,619.93	934.20	1,633.14	689.56
P_{15}	R	1,390.12	615.16	1,438.49	514.59	1,500.16	723.25
	N	1,647.18	530.78	1,584.45	418.56	1,563.20	416.51
P_{16}	R	1,276.87	238.86			1,655.70	432.72
	N	1,900.00	496.76			1,709.98	519.60
P_{17}	R	1,508.08	414.34	1,275.19	389.08	1,746.32	555.36
	N	2,075.00	390.79	1,640.44	355.94	2,066.75	540.79
P_{18}	R	1,487.42	791.48			1,514.85	843.04
	N	1,567.77	825.51			1,338.09	675.29
P_{19}	R	1,172.34	739.67	1,296.11	771.31	1,077.09	579.20
	N	1,862.00	619.42	1,837.65	445.58	1,861.68	291.50
P_{20}	R	1,040.61	473.19	1,258.82	600.25	1,517.22	531.74
	N	1,725.14	768.93	1,883.42	546.82	1,973.29	286.76
P_{21}	R	1,644.62	580.07	1,432.41	690.02	1,665.64	979.91
	N	1,284.81	630.13	1,425.48	940.93	1,622.76	605.87
P_{22}	R	1,230.20	592.52	1,382.43	468.78	1,382.43	468.78
	N	1,724.42	828.64	1,900.98	501.09	1,900.98	501.09
P_{23}	R	1,099.41	462.26	1,322.35	465.59	1,391.23	513.19
	N	1,607.04	716.50	1,528.90	379.87	1,643.48	389.18
	R	1,151.84	372.25	1,213.56	390.99	1,148.25	212.68

Continued on next page

Table A.1 – *Continued from previous page*

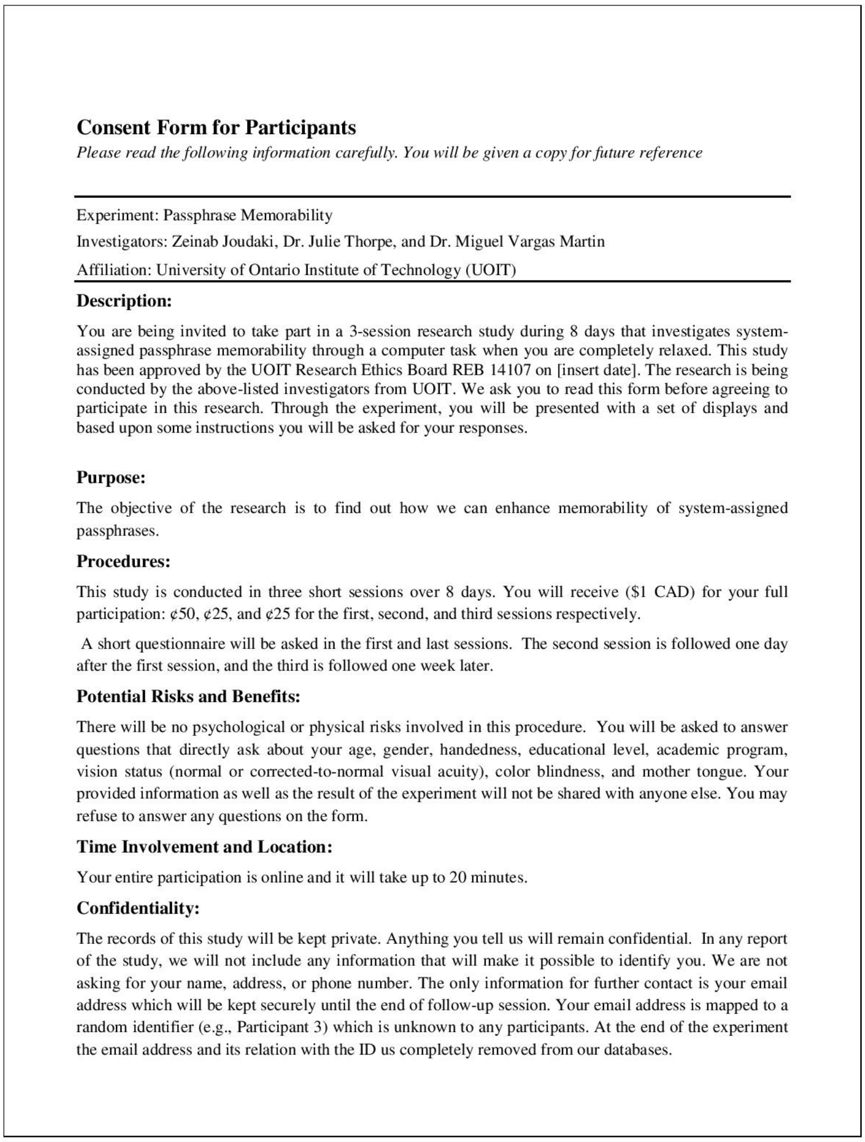
Participant	Type	Testing Session 1		Testing Session 2		Testing Session 3	
		avg	stdev	avg	stdev	avg	stdev
P_{24}	N	1,787.77	511.72	1,587.60	416.88	1,571.15	384.43
P_{25}	R	1,313.32	643.29	800.64	643.59	749.71	303.62
	N	1,764.43	568.14	1,532.13	652.97	2,008.70	143.16
P_{26}	R	1,271.97	665.59	1,406.85	540.06	926.28	338.72
	N	1804.96	733.37	1,666.71	453.27	1887.80	322.67
P_{27}	R	1,162.08	558.93	1,246.57	416.83	1,289.44	448.45
	N	1,809.20	690.43	1,882.28	573.50	1,671.80	559.72
P_{28}	R	1,073.89	386.04	1,115.15	365.98	991.49	366.44
	N	1,689.34	450.01	1,621.55	260.53	1,365.75	348.28
P_{29}	R	1543.90	453.09	1,641.90	546.95	1,312.33	520.34
	N	1,659.90	342.90	1,758.81	661.13	1,497.69	629.25
P_{30}	R	1,552.66	759.94	1,545.95	733.41	1,687.00	641.87
	N	1,452.40	696.14	1,350.75	771.34	1,785.10	643.35

Table A.1 Average and standard deviation of subjects' RT in milliseconds for the different testing sessions.

Appendix B

Implicitly Reinforced Passphrases

B.1 Consent form for Implicitly Reinforced Passphrases



Consent Form for Participants

Please read the following information carefully. You will be given a copy for future reference

Experiment: Passphrase Memorability

Investigators: Zeinab Joudaki, Dr. Julie Thorpe, and Dr. Miguel Vargas Martin

Affiliation: University of Ontario Institute of Technology (UOIT)

Description:

You are being invited to take part in a 3-session research study during 8 days that investigates system-assigned passphrase memorability through a computer task when you are completely relaxed. This study has been approved by the UOIT Research Ethics Board REB 14107 on [insert date]. The research is being conducted by the above-listed investigators from UOIT. We ask you to read this form before agreeing to participate in this research. Through the experiment, you will be presented with a set of displays and based upon some instructions you will be asked for your responses.

Purpose:

The objective of the research is to find out how we can enhance memorability of system-assigned passphrases.

Procedures:

This study is conducted in three short sessions over 8 days. You will receive ($1 CAD) for your full participation: ¢50, ¢25, and ¢25 for the first, second, and third sessions respectively.

A short questionnaire will be asked in the first and last sessions. The second session is followed one day after the first session, and the third is followed one week later.

Potential Risks and Benefits:

There will be no psychological or physical risks involved in this procedure. You will be asked to answer questions that directly ask about your age, gender, handedness, educational level, academic program, vision status (normal or corrected-to-normal visual acuity), color blindness, and mother tongue. Your provided information as well as the result of the experiment will not be shared with anyone else. You may refuse to answer any questions on the form.

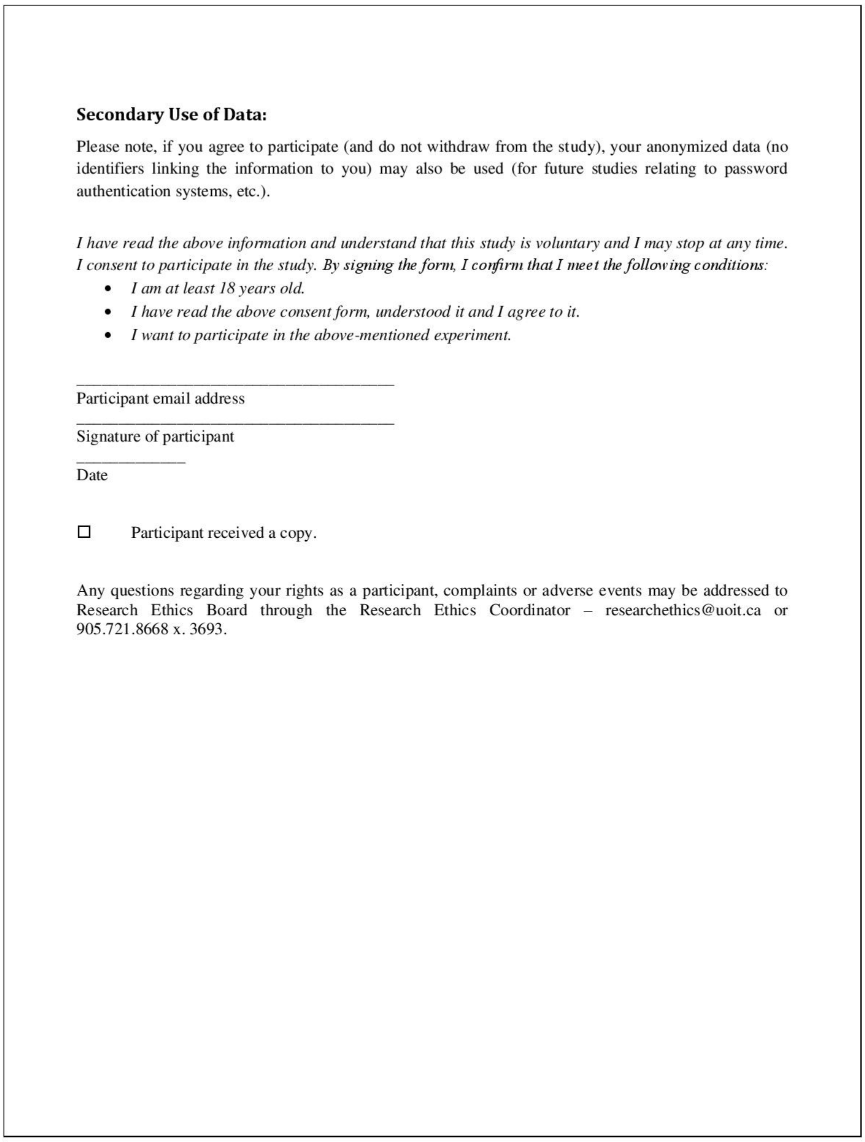
Time Involvement and Location:

Your entire participation is online and it will take up to 20 minutes.

Confidentiality:

The records of this study will be kept private. Anything you tell us will remain confidential. In any report of the study, we will not include any information that will make it possible to identify you. We are not asking for your name, address, or phone number. The only information for further contact is your email address which will be kept securely until the end of follow-up session. Your email address is mapped to a random identifier (e.g., Participant 3) which is unknown to any participants. At the end of the experiment the email address and its relation with the ID us completely removed from our databases.

Fig. B.1 Implicitly Reinforce Passphrases - Consent Form (Page 1 of 2).



Secondary Use of Data:

Please note, if you agree to participate (and do not withdraw from the study), your anonymized data (no identifiers linking the information to you) may also be used (for future studies relating to password authentication systems, etc.).

I have read the above information and understand that this study is voluntary and I may stop at any time. I consent to participate in the study. By signing the form, I confirm that I meet the following conditions:

- *I am at least 18 years old.*
- *I have read the above consent form, understood it and I agree to it.*
- *I want to participate in the above-mentioned experiment.*

____
Participant email address

____
Signature of participant

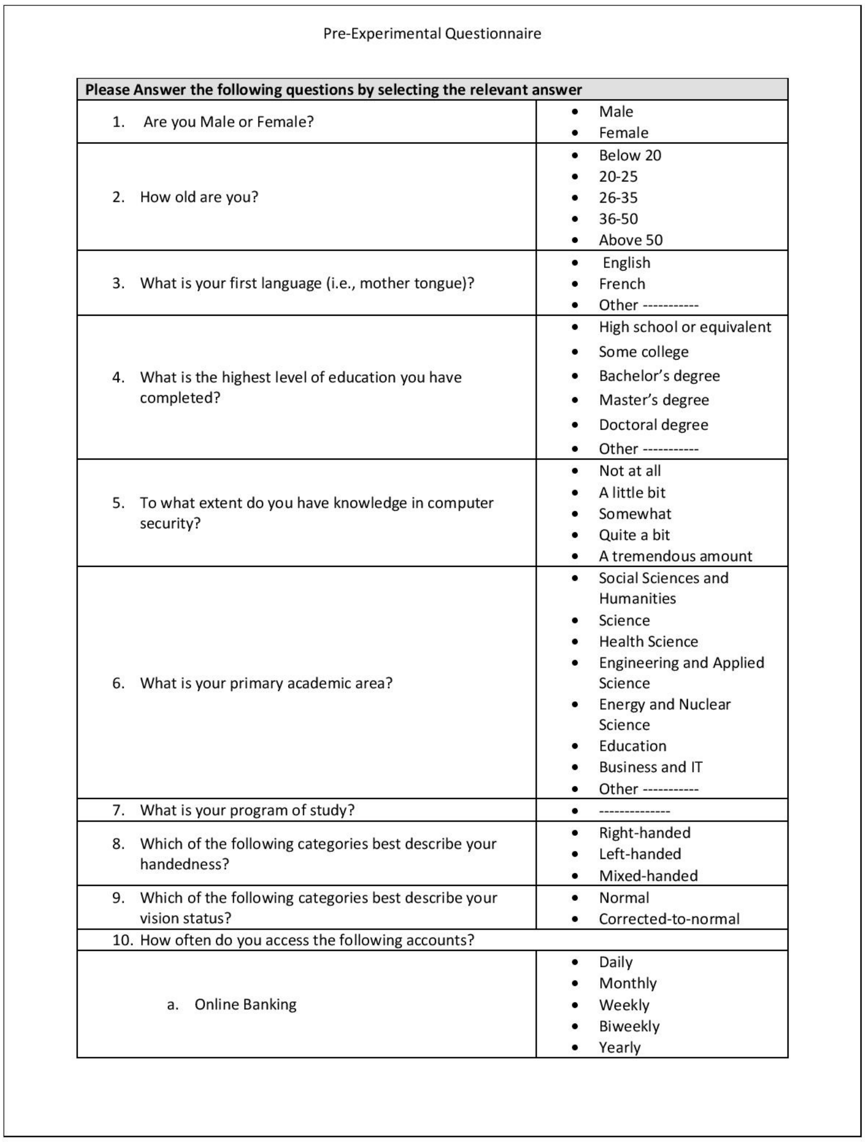
____
Date

□ Participant received a copy.

Any questions regarding your rights as a participant, complaints or adverse events may be addressed to Research Ethics Board through the Research Ethics Coordinator – researchethics@uoit.ca or 905.721.8668 x. 3693.

Fig. B.2 Implicitly Reinforce Passphrases - Consent Form (Page 2 of 2).

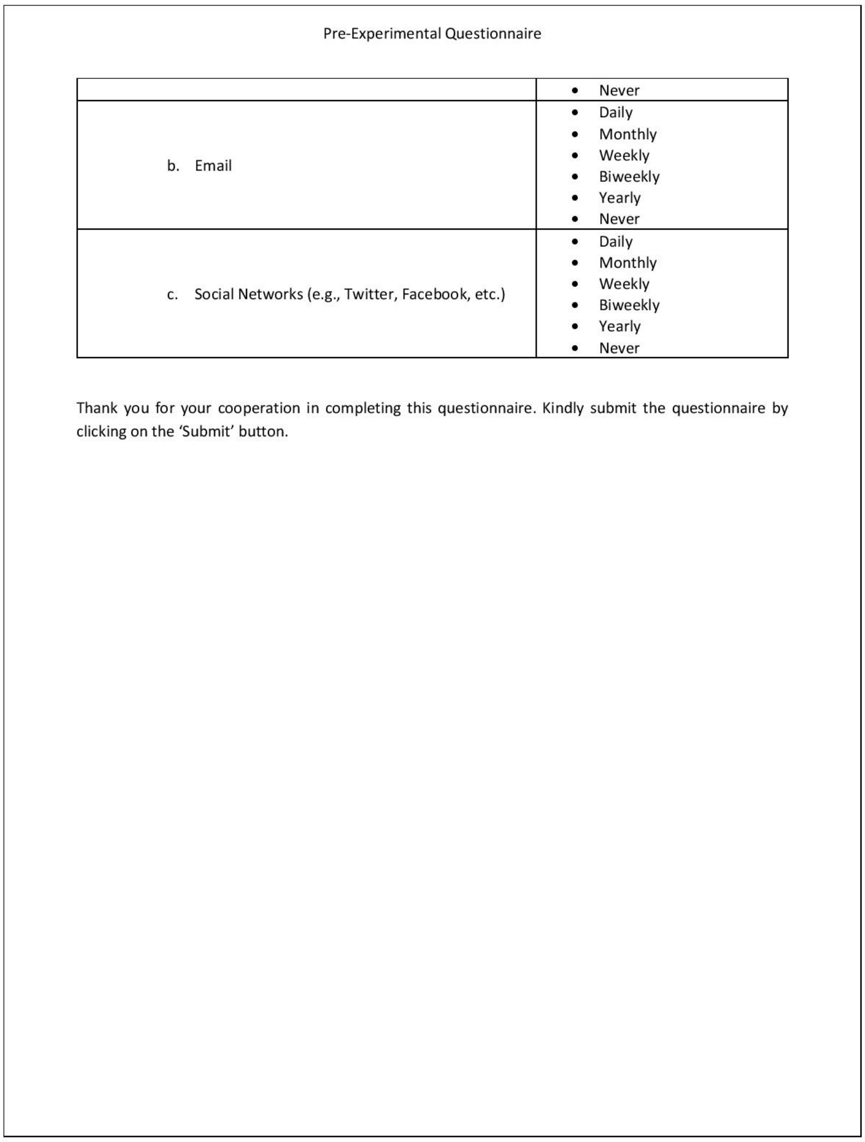
B.2 Questionnaires



Pre-Experimental Questionnaire

Please Answer the following questions by selecting the relevant answer	
1. Are you Male or Female?	• Male • Female
2. How old are you?	• Below 20 • 20-25 • 26-35 • 36-50 • Above 50
3. What is your first language (i.e., mother tongue)?	• English • French • Other -----------
4. What is the highest level of education you have completed?	• High school or equivalent • Some college • Bachelor's degree • Master's degree • Doctoral degree • Other -----------
5. To what extent do you have knowledge in computer security?	• Not at all • A little bit • Somewhat • Quite a bit • A tremendous amount
6. What is your primary academic area?	• Social Sciences and Humanities • Science • Health Science • Engineering and Applied Science • Energy and Nuclear Science • Education • Business and IT • Other -----------
7. What is your program of study?	• --------------
8. Which of the following categories best describe your handedness?	• Right-handed • Left-handed • Mixed-handed
9. Which of the following categories best describe your vision status?	• Normal • Corrected-to-normal
10. How often do you access the following accounts?	
a. Online Banking	• Daily • Monthly • Weekly • Biweekly • Yearly

Fig. B.3 Implicitly Reinforced Passphrase - Pre-experiment questionnaire (Page 1).

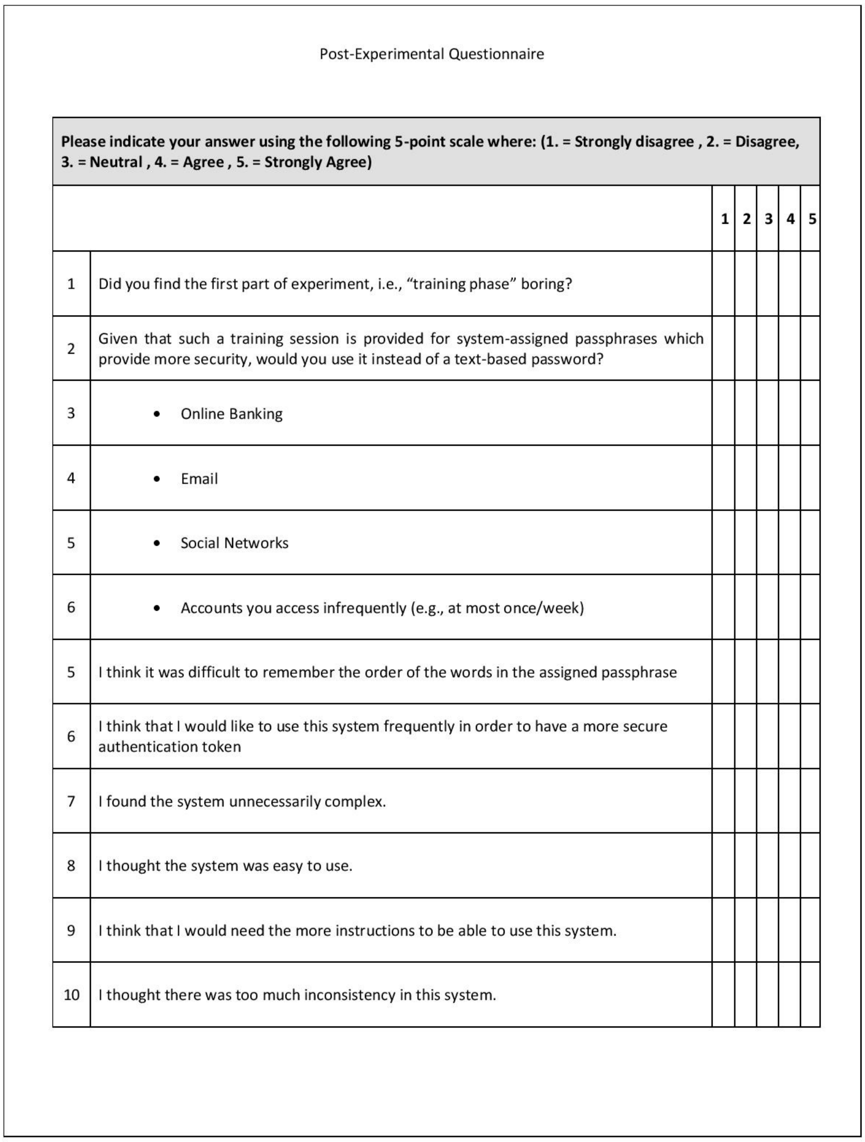


Pre-Experimental Questionnaire

	• Never
b. Email	• Daily • Monthly • Weekly • Biweekly • Yearly • Never
c. Social Networks (e.g., Twitter, Facebook, etc.)	• Daily • Monthly • Weekly • Biweekly • Yearly • Never

Thank you for your cooperation in completing this questionnaire. Kindly submit the questionnaire by clicking on the ‘Submit’ button.

Fig. B.4 Implicitly Reinforced Passphrase - Pre-experiment questionnaire (Page 2).

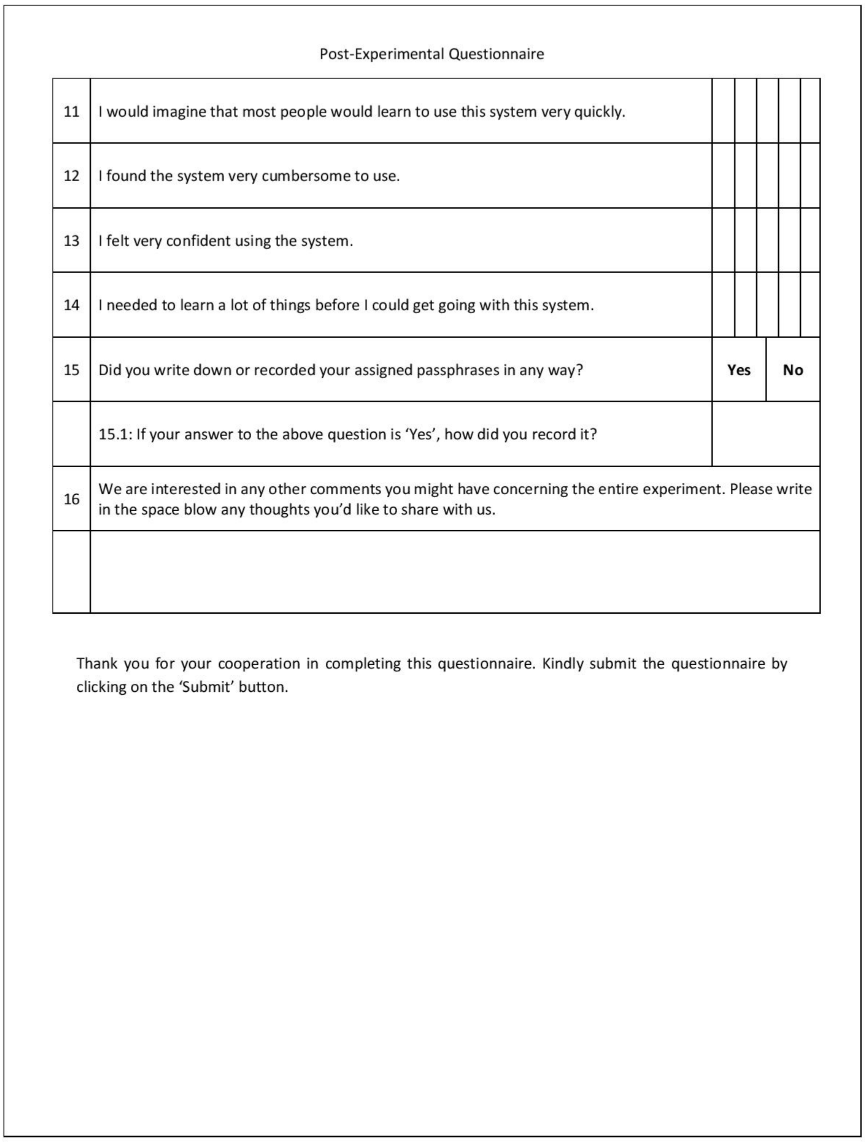


Post-Experimental Questionnaire

Please indicate your answer using the following 5-point scale where: (1. = Strongly disagree , 2. = Disagree, 3. = Neutral , 4. = Agree , 5. = Strongly Agree)

		1	**2**	**3**	**4**	**5**
1	Did you find the first part of experiment, i.e., “training phase” boring?					
2	Given that such a training session is provided for system-assigned passphrases which provide more security, would you use it instead of a text-based password?					
3	• Online Banking					
4	• Email					
5	• Social Networks					
6	• Accounts you access infrequently (e.g., at most once/week)					
5	I think it was difficult to remember the order of the words in the assigned passphrase					
6	I think that I would like to use this system frequently in order to have a more secure authentication token					
7	I found the system unnecessarily complex.					
8	I thought the system was easy to use.					
9	I think that I would need the more instructions to be able to use this system.					
10	I thought there was too much inconsistency in this system.					

Fig. B.5 Implicitly Reinforced Passphrase - Post-experiment questionnaire (Page 1).



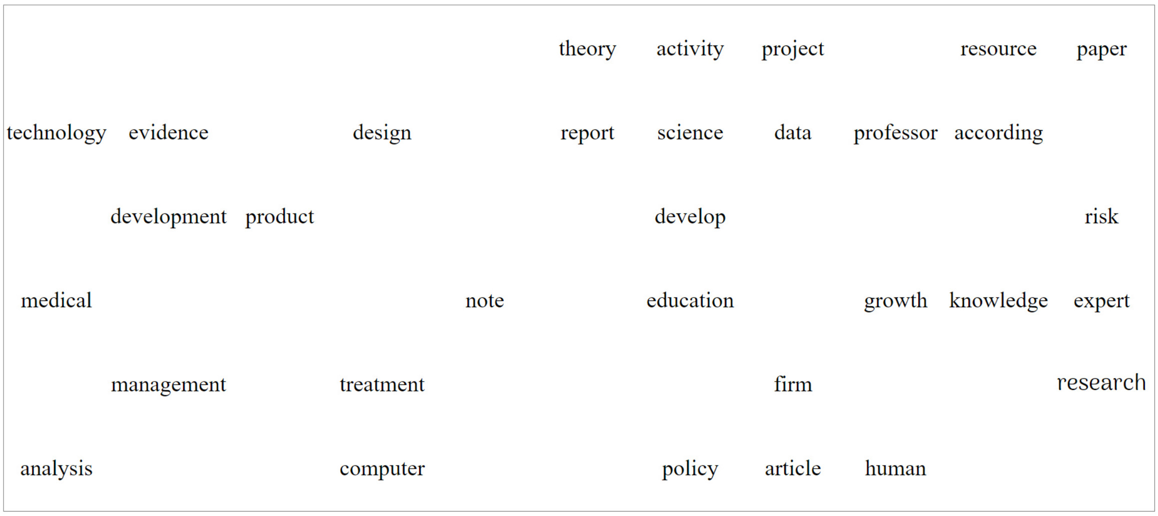
Post-Experimental Questionnaire

11	I would imagine that most people would learn to use this system very quickly.					
12	I found the system very cumbersome to use.					
13	I felt very confident using the system.					
14	I needed to learn a lot of things before I could get going with this system.					
15	Did you write down or recorded your assigned passphrases in any way?	**Yes**		**No**		
	15.1: If your answer to the above question is 'Yes', how did you record it?					
16	We are interested in any other comments you might have concerning the entire experiment. Please write in the space blow any thoughts you'd like to share with us.					

Thank you for your cooperation in completing this questionnaire. Kindly submit the questionnaire by clicking on the 'Submit' button.

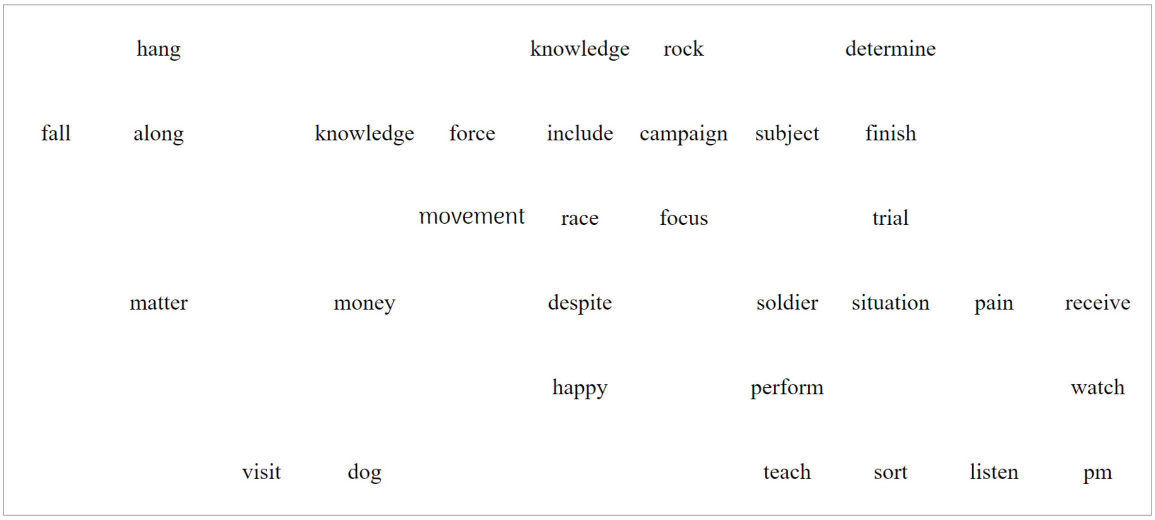
Fig. B.6 Implicitly Reinforced Passphrase - Post-experiment questionnaire (Page 2).

B.3 Screenshots of Sample CC-SP and CC displays



					theory	activity	project		resource	paper
technology	evidence		design		report	science	data	professor	according	
	development	product				develop				risk
medical				note		education		growth	knowledge	expert
	management		treatment				firm			research
analysis			computer			policy	article	human		

Fig. B.7 Sample CC-SP display for Implicitly Reinforced Passphrases Experiment. The target word is ‘research’.



	hang				knowledge	rock		determine		
fall	along		knowledge	force	include	campaign	subject	finish		
				movement	race	focus		trial		
	matter		money		despite		soldier	situation	pain	receive
					happy		perform			watch
		visit	dog				teach	sort	listen	pm

Fig. B.8 Sample CC display for Implicitly Reinforced Passphrases Experiment. The target word is ‘movement’.